UiO : Det juridiske fakultet

Domfeltes innsynsrett og kontroll ved innsynsnekt i Infoflyt-systemet

Jf. Prop. 120L (2013-2014)

Kandidatnummer: 587

Leveringsfrist: 25.11.2014

Antall ord: 16724

Innholdsfortegnelse

1 INNLEDNING 1

1.1 Tema, problemstilling og aktualitet 1
1.2 Nærmere om behandling av personopplysninger 2
1.3 Metode og rettskilder 4
1.3.1 Metode 4
1.3.2 Gjeldende regulering av Infoflyt-systemet 4
1.3.3 Rettskildebildet etter Prop. 120L (2013-2014) 5
1.4 Avgrensning 6
1.5 Videre disposisjon 7

2 INFOFLYT-SYSTEMET - HISTORIEN, REGISTRERINGEN OG RETTSGRUNNLAG ETTER GJELDENDE RETT 7

2.1 Innledning 7
2.2 Infoflyt-systemets historie og kritikk 8
2.2.1 Nærmere om Infoflyts-utvalgets funn 9
2.3 Kort redegjørelse for regulering av Infoflyt-systemet etter gjeldende rett 12
2.3.1 Innledning 12
2.3.2 Formål og vilkår for registrering etter gjeldende rett 12
2.3.3 Registreringen 13
2.3.4 Kort om retten til informasjon og innsyn etter personopplysningsloven 13
2.3.5 Kort om den registrertes klage- og kontrollmuligheter 15

3 REGLENE OM INNSYN JF. PROP. 120 L (2013-2014) 16

3.1 Innledning 16
3.2 Hensyn som taler for og mot innsyn 16
3.3 Forutsetning for effektiv innsynsrett, kort om informasjonsplikten 17
3.4 Hva innebærer retten til å be om innsyn og hvem gjelder den for? 19
3.5 Redegjørelse av unntakene fra innsynsrett 20
3.5.1 Unntak for innsynsrett for å ivareta formålene med behandling av personopplysninger i Infoflyt-systemet 20
3.5.2 Unntak for innsynsrett for å ivareta nasjonal og offentlig sikkerhet 26
3.5.3 Unntak for innsynsnekt når opplysningene er utlevert fra PST 30
3.5.4 Svar på innsynsbegjæring 32
3.6 Innsynsregelen oppsummeres og settes opp mot gjeldende rett 33

4 KONTROLLMULIGHETER OG KLAGEADGANG 36

4.1 Innledning 36
4.2 Datatilsynets kontroll og virkemidler jf. Prop. 120 L (2-13-2014) 36
4.2.1 Rekkevidden av Datatilsynets kompetanse for tilsyn med Infoflyt-systemet 37
4.2.2 Har Datatilsynet påleggskompetanse? 40
4.3 Andre kontroll- og klagemuligheter 43
4.3.1 Innledning 43
4.3.2 Sivilombudsmannens kontroll 43
4.3.3 Klageadgang til overordnet forvaltningsorgan 44
4.3.4 Domstolsprøving 45
4.4 Kontrollmuligheter og klageadgang i lovforslaget oppsummeres og settes opp mot gjeldende rett 48

5 AVSLUTTENDE BEMERKNINGER 49

6 LITTERATURLISTE 51

6.1 Lov 51
6.1.1 Opphevet lov 52
6.2 Forskrift, retningslinjer og rundskriv 52
6.3 Traktater og direktiver 52
6.4 Forarbeider 53
6.4.1 Proposisjoner 53
6.4.2 Rapporter 53
6.4.3 Norges offentlige utredninger (NOU) 53
6.5 Rettspraksis 54
6.5.1 Høyesterett 54
6.5.2 Den Europeiske menneskerettigehetsdomstol (EMD) 54
6.6 Andre myndigheters praksis 54
6.7 Internasjonale rapporter 55
6.8 Litteratur 55
6.8.1 Bøker 55
6.8.2 Nettdokumenter 56
6.8.3 Annet 56
6.8.4 Samtaler 57

1 Innledning

1.1 Tema, problemstilling og aktualitet

Infoflyt-systemet er et informasjonsutvekslingssystem mellom kriminalomsorgen[1] og politiet og påtalemyndigheten i særlig alvorlige saker. Systemet kommer i tillegg til kriminalomsorgens ordinære datasystem Kompis, der alle innsatte i norske fengsler er registrert. I Infoflyt-systemet lagres personopplysninger om den registrerte, som er samlet inn av både politiet og kriminalomsorgen. Formålet med registreringen i Infoflyt-systemet er å sette kriminalomsorgen i bedre stand til å foreta risikovurderinger av den enkelte innsatte og eventuelle nettverk vedkommende er en del av, samt å være et verktøy for politiet til å avdekke kriminalitet under straffegjennomføring og forebygge ny kriminalitet.[2] Risikovurderingene som kriminalomsorgen foretar på bakgrunn av opplysninger fra Infoflyt-systemet, danner videre grunnlag for vedtak om eksempelvis soningsoverføring til andre fengsler eller lavere sikkerhetsnivå, isolasjon, permisjoner og prøveløslatelser[3].

For den registrerte kan det ha betydning å få innsyn i hvilke opplysninger som er registrert om han i Infoflyt-systemet. For det første setter innsynsretten den registrerte i stand til å imøtegå de opplysningene som er registrert om han. Kontradiksjon er et grunnleggende rettssikkerhetsprinsipp som beskytter mot overgrep og vilkårlighet fra myndighetenes side.[4] Hovedbegrunnelsen for kontradiksjon er å sikre riktig avgjørelse, idet holdbarheten av et argument først kan vurderes når det har vært gitt anledning til å imøtegå det.[5]

For det andre er innsynsretten viktig for å kunne ivareta den innsattes personvern. Personvernkommisjonen definerer personvern vidt ved at begrepet omfatter både vernet av privatlivets fred, den enkeltes personlige integritet, og personopplysningsvernet som angår individets

[1] Kriminalomsorgen er delt i tre nivåer med Kriminalomsorgsdirektoratet (KDI) øverst. Den består videre av fem regionadministrasjoner, de lokale fengslene og friomsorgskontorene, samt Kriminalomsorgens utdanningssenter (KRUS) som er direkte underlagt direktoratet. Jf. regjerningen.no: kriminalomsorgsdirektoratet.

[2] Jf. Rundskriv fra Kriminalomsorgens sentrale forvaltning KSF 2/2005 om INFOFLYT – særskilt saksbehandlingsinstruks (heretter KSF 2/2005)

[3] En innsatt kan vurderes for løslatelse på prøve når vedkommende har sonet to tredjedeler av straffen, jf. straffegjennomføringsloven (lov av 18.5.2001 nr.21) § 42. Løslatelse etter 2/3-tid er vanlig praksis i Norge.

[4] Jf. Eckhoff og Smith, 2009, s. 58-59

[5] Jf. Robberstad, 2009, s. 9-11

rett til å ha oversikt og kontroll over behandling av opplysninger om seg selv.[6] For den innsatte har de nevnte rettighetene nær sammenheng, da situasjonen under soning består av lite privatliv og hans personlige integritet i stor grad avhenger av et godt personopplysningsvern. Personvernbegrepet vil i denne oppgaven derfor omhandle både vern av privatlivets fred og av personopplysningsvernet. Hvor stort et personverninngrep er avhenger av hvor og hvordan det skjer, om det strekker ut i tid og omfanget av inngrepet.[7] Det som skiller Infoflyt-systemet fra annen behandling av personopplysninger, er at innsamlingen og utvekslingen av opplysninger i stor grad foregår skjult og i et omfang den registrerte ikke får kunnskap om.

Bakgrunnen for denne oppgaven er at det har vært rettet kritikk mot Infoflyt-systemet, som har ledet frem til lovforslaget Prop. 120 L (2013-2014) «Endringer i straffegjennomføringsloven mv. (Infoflytsystemet mv.)». Hovedproblemstillingen for oppgaven er hvordan retten til personvern og kontradiksjon vil bli ivaretatt i Infoflyt-systemet dersom regelverket endres i medhold av Prop. 120 L (2013-2014). Problemstillingen besvares ved å undersøke den domfeltes innsynsrett og klagemuligheter, samt andre ordninger for kontroll. For å finne ut om lovforslaget faktisk vil føre til en endring for den domfelte, vil jeg også trekke paralleller fra lovforslaget til gjeldende rett. Oppgavens aktualitet ligger i at lovforslaget er i siste fase før vedtakelse, der Stortingskomiteen har frist til avgivelse av innstilling den 2.12.2014.

1.2 Nærmere om behandling av personopplysninger

Kjernen i Infoflyt-systemet er behandling av personopplysninger. Med *behandling av personopplysninger* menes all bruk av personopplysninger, «f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter», jf. personopplysningsloven[8] § 2 nr. 2 og straffegjennomføringsloven[9] § 4a.

Det er i NOU 2009:1 *Individ og Integritet* lagt til grunn en vid tolkning av hva som menes med personopplysning, i tråd med personverndirektivet.[10] En *personopplysning* er «opplysninger og vurderinger som kan knyttes til en enkeltperson», jf. popplyl. § 2 nr. 1. Med *opplys-*

[6] Jf. NOU 2009: 1 Individ og integritet s. 32

[7] Se Bruce og Haugland, 2014, s. 26

[8] Personopplysningloven, lov av 14.4.2000 nr. 31 (heretter popplyl.)

[9] Straffegjennomføringsloven, lov av 18.5.2001 nr. 21 (heretter strgjfl.)

[10] Jf. NOU 2009:1 s. 47

ning menes faktabaserte former for data knyttet til en person, som navn og adresse. Det er ikke et krav at opplysningen er sann eller bevist.[11] *Vurderinger* er sammensatte former for data, og vil ofte være basert på én eller flere opplysninger.[12] I Infoflyt-sammenheng vil en vurdering for eksempel kunne være at «NN er voldelig og må behandles med varsomhet». Også opptak av telefonsamtale og videoopptak omfattes av definisjonen.[13] Tilknytningen kan være både direkte, som personens navn, eller indirekte, som den innsattes fangenummer.

Personopplysningsloven skiller mellom vanlige personopplysninger og *sensitive personopplysninger*. Hva som er sensitive, og dermed beskyttelsesverdige, opplysninger kan være subjektivt forskjellig fra person til person. Personopplysningsloven har imidlertid listet opp en rekke opplysninger som skal ansees som sensitive etter loven i § 2 nr. 8[14], og som dermed skal behandles mer varsomt, jf. § 11 jf. § 9. Personopplysninger som registreres i Infoflyt-systemet vil etter dette som regel være sensitive, jf. bokstav b.

Personopplysningsloven omfatter behandling av personopplysninger ved bruk av elektroniske hjelpemidler som f. eks datamaskin, jf. § 3, samt annen behandling der personopplysningene «inngår eller skal inngå i et personregister», jf. § 3 (1) litra b. Sistnevnte *register* er altså ikke elektronisk, men må kjennetegnes av at «fortegnelsene mv. er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen», jf. § 2 nr. 3. Infoflyt-systemet benytter både elektronisk og manuell systematisk registrering av personopplysninger. Etter dette omfattes således all behandling av personopplysninger i Infoflyt-systemet av personopplysningslovens definisjon av registering, og må således i utgangspunktet følge de krav som loven oppstiller for slik behandling.

[11] Jf. NOU 2009:1 s. 47

[12] Jf. NOU 2009: 1 s. 47

[13] Jf. NOU 2009:1 s. 47

[14] Popplyl. § 2 nr. 8: «Sensitive personopplysninger: personopplysninger om: a) rasemessig eller etnisk bakgrunn eller politisk, filosofisk eller religiøs oppfatning, b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, c) helseforhold, d) seksuelle forhold, e) medlemskap i fagforeninger.»

1.3 Metode og rettskilder

1.3.1 Metode

Til grunn for tolkning av lovforslaget om regulering av Infoflyt-systemet anvendes tradisjonell juridisk metode.[15] I tillegg til å tilegne meg kunnskap om Infoflyt-systemet gjennom de tradisjonelle rettskildene som omtales nedenfor, har jeg også vært i samtale med henholdsvis kriminalomsorgens Region øst og Datatilsynet. Det er referert fra samtalene der det er ansett relevant for å belyse problemstillingen.

Tema for oppgaven er innsynsreglene i lovforslag Prop. 120 (2013-20014). For å finne ut hvordan lovforslaget vil få utslag for den registrerte, behandles lovforslaget som om det er formelt vedtatt. Problemstillingen legger også opp til en sammenligning med gjeldende rettstilstand. Ved presentasjonen av rettskildene nedenfor følger derfor først en gjennomgang av gjeldene regulering av Infoflyt-systemet der det redegjøres for lov, forskrift og rundskriv, og deretter følger en redegjørelse av hvordan rettskildebildet vil bli ved eventuell vedtakelse av lovforslag Prop. 120 L (2013-2014).

1.3.2 Gjeldende regulering av Infoflyt-systemet

Selve registreringen i Infoflyt-systemet reguleres av saksbehandlingsinstruks KSF 2/2005, som er forankret i rundskriv G-3/2005 om Informasjonsutveksling mellom kriminalomsorgen og politiet/påtalemyndigheten. Da Infoflyt-systemet ble opprettet var det meningen at systemet skulle ha hjemmel i og reguleres av rundskrivene. Legalitetsprinsippet[16] krever imidlertid at inngrep foretas ved hjemmel i lov, og etter gjeldende rett kan derfor ikke praktiseringen av Infoflyt-systemet gå lengre enn det lov om behandling av personopplysninger (personopplysningsloven) av 14.4.2000 nr. 31 (heretter popplyl.), [17] med tilhørende forskrift, tillater.

---

[15] Jf. Eckhoffs rettskildelære i Helgesen, 2001.

[16] Legalitetsprinsippet gjelder all myndighetsutøvelse og beskytter borgerne mot vilkårlig maktbruk fra myndighetenes side. Prinsippet innebærer at myndigheten må ha hjemmel i lov for å kunne gjøre inngrep i en persons rettssfære, og stiller krav om hjemmelens klarhet. Jo mer inngripende et tiltak er, jo strengere krav stilles til behandlingen og til hjemmelens krav. Se også Rt. 1975 s. 931 og Rt. 1995 s.530.

[17] Personopplysningsloven bygger på personverndirektivet i EU, direktiv 95/46/EF, av 24.10.1995

1.3.3 Rettskildebildet etter Prop. 120L (2013-2014)

Lovforslagene i Prop. 120L (2013-2014) vil ved eventuell vedtakelse stå som et eget kapittel 1 b i lov om gjennomføring av straff (straffegjennomføringsloven) av 18.5.2001 nr. 21 (heretter strgjfl.), og erstatte rundskrivene KSF 2/2005 og G3/2005. Det er foreløpig ikke lagt fram forslag til forskrift til lov om Infoflyt-systemet.

Det er straffegjennomføringsloven med forskrift og rundskriv som regulerer kriminalomsorgens gjennomføring av fengselsstraff. Straffegjennomføringsloven er en del av forvaltningsretten og kriminalomsorgen følger således de alminnelige regler for saksbehandling i lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) av 10.2.1967 (heretter fvl.). Politiets bruk av personopplysninger reguleres av lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) av 28.5.2010 nr. 16 (heretter polregl.). Ved eventuell vedtakelse av lovforslaget vil Infoflyt-systemet gjelde for de personopplysninger som politiet utleverer til kriminalomsorgen. Den Europeiske menneskerettighetskonvensjonen 4.11.1950 (EMK), gjelder som norsk rett da den er inkorporert gjennom lov om styrking av menneskerettighetenes stilling i norsk rett av 21.5.1999 nr. 30 (heretter mnskrl.). Utover dette vil relevant lovgivning redegjøres for der det er nødvendig.

Ved eventuell vedtakelse av lovforslagene i Prop. 120 L (2013-2014) vil Infoflyt-utvalgets rapport av 15. mai 2012 (heretter Rapport 2012) gjelde som forarbeid. I drøftelsen av lovforslaget får Infoflyt-utvalgets rapport utfyllende betydning der lovforslaget er kortfattet eller taust. Utover rapporten vil øvrige relevante forarbeider trekkes inn der det er nødvendig for å utdype eller belyse lovforslaget.

Det er begrenset med rettspraksis som omhandler Infoflyt-systemet. Så vidt meg bekjent er Infoflyt-saker verken behandlet i Høyesterett eller underretter. Det foreligger imidlertid noe praksis om Infoflyt-systemet fra Sivilombudsmannen og Datatilsynet. Rettspraksis fra Høyesterett som ikke direkte omhandler Infoflyt-systemet, men som har relevans for å belyse problemstillingen, vil bli trukket frem der det er nødvendig. Praksis fra Den Europeiske menneskerettighetsdomstol (EMD) vil benyttes i drøftingen av lovforslaget. Videre vil en rapport

fra FNs arbeidsgruppe mot vilkårlig fengsling trekkes frem, der spørsmål om Infoflyt-systemet ble behandlet.[18]

Infoflyt-systemet er omtalt i Birgittes Langset Storviks bok «Straffegjennomføringsloven» fra 2003 (oppdatert 2011). Jeg er ikke kjent med at Infoflyt-systemet behandles i juridisk litteratur utover det. Annen relevant juridisk litteratur vil imidlertid bli benyttet til å besvare problemstillingen der det er relevant.

1.4 Avgrensning

Deler av kritikken som har vært reist mot Infoflyt-systemet har dreid seg om at det ikke har foreligget et tilstrekkelig klart hjemmelsgrunnlag for behandling av personopplysninger, jf. legalitetsprinsippet. Det avgrenses imidlertid mot å drøfte hvorvidt foreliggende lovforslag er i tråd med dette prinsippet.

Oppgavens problemstilling angår innsynsrett i Infoflyt-systemet, og det avgrenses derfor mot problemstillinger tilknyttet kriminalomsorgens og politiets bruk av opplysningene. Forvaltningens bruk av opplysningene vil imidlertid bli trukket frem for å belyse betydningen av innsynsrett for den registrerte.

Oppgaven omhandler innsynsretten til domfelte. Med ordet domfelt menes i denne oppgaven personer med rettskraftig dom, som soner i norske fengsel. Det avgrenses dermed mot varetekstfengsledes innsynsrett. Varetekstfengslede er i en annen situasjon enn den domfelte på flere måter. De fleste er fengslet for en kortere periode, mens en domfelt som er aktuell for Infoflyt-registrering gjerne har en lengre dom. Videre kan begrunnelsen for varetektsfengslingen f.eks. være etterforskningshensyn mens det for den domfelte har rettskraftig dom. Den varetektsfengslede har også krav på advokat under straffesaken, noe den domfelte ikke har mv. Da situasjon og hensyn er så vidt ulike, avgrenses det derfor mot varetekstfengslede. Begrepene domfelt og innsatt vil bli brukt om hverandre.

[18] Rapport A/HRC/7/4/Add.2 av 11.10.2007 Rapport fra FNs arbeidsgruppe mot vilkårlig fengsling (Working Group on Arbitrary Detention) Arbeidsgruppen ble opprettet av FNs menneskerettighetsråd (UNHRC) i 1991, og det står i arbeidsgruppens mandat å overvåke og arbeider mot vilkårlig frihetsberøvelse, jf. SP-konvensjonen art. 9 nr. 1.

I tillegg til registrering av opplysninger om domfelte omhandler lovforslaget registrering av opplysninger om personer som er i kontakt med den innsatte.[19] Tredjepersoners rett til innsyn vil imidlertid ikke behandles i oppgaven da det reiser så vidt forskjellige problemstillinger og hensyn enn for domfelte.

Det faller videre utenfor problemstillingen å drøfte om selve registreringen i Infoflyt-systemet kan påklages da det ikke umiddelbart får betydning for innsynsretten.

1.5 Videre disposisjon

Oppgaven er i det videre delt i tre. Del 2 omhandler Infoflyt-systemet og gjeldende rett, del 3 redegjør og drøfter hvordan innsynsrett er regulert i lovforslaget, og del 4 redegjør og drøfter adgang til klage og kontroll med vedtak om innsynsnekt. Hver del innledes med en kort redegjørelse for oppbygging, og avsluttes med en oppsummering og en vurdering av lovforslaget opp mot gjeldende rett. I del 5 følger avsluttende bemerkninger.

2 Infoflyt-systemet - Historien, registreringen og rettsgrunnlag etter gjeldende rett

2.1 Innledning

Fra første registrering i 2004 og frem til januar 2011 har ca. 190 innsatte og domfelte vært registrert i systemet, og per 1.1.2011 var det ca. 50 aktive saker registrert i Infoflyt-systemet.[20] Antallet innsatte i norske fengsler er ca. 3700,[21] og det er dermed et fåtall innsatte som er registrert i Infoflyt-systemet. For å forstå hvordan Infoflyt-systemet fungerer, og for å få et bakteppe for behovet for lovforslaget, følger nedenfor en redegjørelse for Infoflyt-systemets historie og en kort redegjørelse for selve registreringen. Til slutt følger en redegjørelse av grunnlaget for Infoflyt-systemet etter gjeldende rett.

[19] Se eksempelvis Prop. 120 L (2013-2014) strgjfl. § 4f (4) og § 4g (2) bokstav d.
[20] Jf. Prop. 120L (2013-2014) s. 25
[21] Jf. kriminalomsorgen.no

2.2 Infoflyt-systemets historie og kritikk

Før Infoflyt-systemet[22] ble opprettet var utvekslingen av opplysninger mellom kriminalomsorgen og politiet uformell og lite ensartet.[23] I 1998 utarbeidet Justisdepartementet en strategi for et informasjonsutvekslingssystem (Infoflyt), og utprøvingen av dette startet høsten 2002. Første Infoflyt-sak ble behandlet og registrert av Kriminalomsorgens sentrale forvaltning (KSF)[24] høsten 2004.[25] Våren 2005 kom Rundskriv G-3/2005 om informasjonsutvekslingen mellom politiet/påtalemyndigheten og kriminalomsorgen, utarbeidet av Justis- og politidepartementet. Rundskrivet forutsatte en særskilt saksbehandlingsinstruks om Infoflyt-systemet som ble formalisert i rundskriv KSF 2/2005, utarbeidet av KSF, Riksadvokaten, Politidirektoratet og Politiets sikkerhetstjeneste.[26] Den registrertes innsynsrett fulgte etter dette strgjfl. § 7(1) bokstav c, der det kan gjøres unntak fra innsynsretten for de tilfeller det er utilrådelig at parten får kjennskap til opplysningene. Av KSF 2/2005 gikk det frem at registrering i Infoflyt-systemet i seg selv kunne danne grunnlag for innsynsnekt.

Det har vært rettet kritikk mot Infoflyt-systemet både nasjonalt og internasjonalt. Kritikken har hovedsakelig omhandlet hjemmelsgrunnlaget, brudd på personvernlovgivningen og manglende kontradiksjonsadgang. FNs arbeidsgruppe mot vilkårlig fengsling besøkte norske fengsler våren 2007, og skrev på bakgrunn av dette en rapport A/HRC/7/4/Add.2 av 11.10.2007.[27] Arbeidsgruppen mente at Infoflyt-systemet hadde et kontradiktorisk underskudd ved at Sivilombudsmannen var det eneste utenforliggende kontrollorgan som fikk innsyn i opplysningene, ettersom også domstolen var avslått innsynsrett.[28] Sivilombudsmannen har kritisert kriminalomsorgens praktisering av Infoflyt-systemet ved flere anledninger.[29] Mest relevant for den domfeltes innsynsrett er ombudsmannssak 2007/264 der Sivilombudsmannen kritiserte krimi-

[22] Av hensyn til variasjon i språkbruk benyttes både begrepene «Infoflyt-systemet», «Infoflyt» og «systemet» når Infoflyt-systemet beskrives og drøftes.

[23] Jf. INFOFLYT Informasjonsutveksling mellom politiet og kriminalomsorgen i saker med alvorlig kriminalitet og høy risiko. Rapport av 15. mai 2012 (heretter Rapport 2012) s. 16

[24] Tidligere var KSF øverste organ i kriminalomsorgen. Dette ble endret etter en omstrukturering i 2013 da det ble opprettet et eget direktorat for kriminalomsorgen, Kriminalomsorgsdirektoratet (KDI).

[25] Jf. Rapport 2012 s. 16

[26] Jf. Rapport 2012 s. 16

[27] Arbeidsgruppen ble opprettet av FNs menneskerettighetsråd (UNHRC) i 1991, og det står i arbeidsgruppens mandat å overvåke og arbeider mot vilkårlig frihetsberøvelse, jf. SP-konvensjonen art. 9 nr. 1.

[28] A/HRC/7/4/Add.2 §§ 83-90. Rapporten blir kommentert nærmere under pkt. 2.2.1.

[29] Se eksempelvis sakene 2007/2274, 2007/497, 2007/264, 2006/1502

nalomsorgens praktisering av innsynsreglene i Infoflytsystemet. Det kom frem av denne saken at kriminalomsorgen, med grunnlag i KSF 2/2005 og strgjfl. § 7(1) bokstav c, kategorisk avslo innsynsbegjæringer på bakgrunn av at vedkommende var registrert i Infoflyt. I tillegg til å kritisere en manglende konkret vurdering mente Sivilombudsmannen at det ikke var gitt tilstrekkelig begrunnelse for avslaget. I brev av 5.6.2009 (sak 2007/2274) stilte Sivilombudsmannen en rekke spørsmål til Justis- og politidepartementet knyttet til Infoflyt-systemet. [30] Ombudsmannen uttalte at registrering i Infoflyt-systemet kunne utgjøre et inngrep i privatlivets fred, jf. EMK art. 8, og at det var usikkert om det rettslige grunnlaget for Infoflyt-systemet var tilstrekkelig klart i henhold til legalitetsprinsippet. I tillegg til denne kritikken vises det også til Datatilsynets kontrollrapport av 25.1.2008 som avdekket en rekke brudd på personvernlovgivningen ved behandling av personopplysninger i kriminalomsorgen. Dette tilsynet gjaldt ikke Infoflyt-systemet spesielt, men funnene fra tilsynet understreket behovet for en bedre regulering av behandling av personopplysninger i kriminalomsorgen. Datatilsynets kontrollrapport dannet bl.a. grunnlag for at straffegjennomføringsloven fikk et eget kapittel om behandling av personopplysninger i kriminalomsorgen, kapittel 1a. [31]

På bakgrunn av denne kritikken satte Justis- og politidepartementet i 2010 ned et utvalg, Infoflyt-utvalget, for å utrede systemet. [32] Rapporten med lovforslag ble levert 15.5.2012, for så å bli sendt på høring. I juni 2014 forelå lovforslaget Prop. 120 L (2013-2014).

2.2.1 Nærmere om Infoflyts-utvalgets funn

Det lå i utvalgets mandat å kartlegge og vurdere gjeldende praksis for Infoflyt, samt foreslå regler og saksbehandlingsrutiner for behandling av personopplysninger i Infoflyt.[33] Infoflyt-utvalget la til grunn at Infoflyt-systemet representerte et inngrep i den registrertes personvern, og et av hovedfunnene i rapporten var at strgjfl. kapittel 1a ikke gav tilstrekkelig klart hjemmelsgrunnlag for Infoflyt-systemet.[34] Utvalget vurderte deretter Infoflyt-systemet ut i fra personopplysningsloven. Ettersom personopplysningsloven ikke er tilpasset kriminalomsorgens

[30] Jf. brev av 5.juni 2009 (2007/2274) i Rapport 2012 s. 17

[31] Kapittel 1a om kriminalomsorgens behandling av personopplysninger ble lagt til strgjfl. den 17.12.2010, jf. Prop. 151 L (2009-2010)

[32] Jf. Prop. 120L (2013-2014) s. 11

[33] Jf. Rapport 2012 s.6

[34] Jf. Rapport 2012 s. 73-85

og politiets behov ved bruk av Infoflyt-systemet, foreslo Infoflyt-utvalget et nytt kapittel 1b i straffegjennomføringsloven med forskrift.[35]

I forbindelse med rapporten 2012 gikk Infoflyt-utvalget gjennom et tilfeldig utvalg saker fra 2004-2009, alle saker fra 2009, samt et utvalg saker der det forelå forvaltningsklager. [36] Det kom frem at det var svært ulike rutiner hva gjaldt informasjonssikkerhet[37] og behandlingsrutiner i de ulike fengslene.[38] Av hensyn til leserens forståelse av hvordan Infoflyt-systemet fungerer og viktigheten av innsynsrett for den innsatte vil noen av funnene fra utvalgets rapport gjennomgås nedenfor.

Infoflyt-systemet består av både elektroniske og manuelle mapper.[39] I de elektroniske mappene registreres kun data over inngående og utgående dokumenter, og selve dokumentet finnes i det manuelle arkivet. Hovedarkivet er hos Justis- og beredskapsdepartementet, og det lokale fengselet holder en kopi av mappen mens saken er aktiv[40]. Et av funnene til utvalget var at det syntes å mangle systematikk i kopiene og rutiner for oppdatering av lokal kopi.[41] De pekte på at slik manglende systematikk kan være problematisk, da det medfører risiko for at det kan være opplysninger i en kopi som ikke er i originalen og motsatt. Videre fant de at det forelå egne lokale rutiner for behandling av mappene, samt at skriftlige rutiner ikke alltid ble fulgt.[42] De ovennevnte manglene får betydning for opplysningskvaliteten[43] i den enkelte Infoflyt-mappe, og således også betydning for kvaliteten på kriminalomsorgens risikovurderinger når det skal fattes enkeltvedtak.

---

[35] Jf. «Nytt kapittel 1 b. Særlig om behandling om behandling av personopplysninger», Rapport 2012 s. 104 flg.

[36] Jf. Rapport 2012 s. 65

[37] Informasjonssikkerhet er et grunnleggende personvernprinsipp som bl.a. følger av personverndirektivet § 17 og som reguleres i popplyl. §§ 12-15 og kapittel 2 i personopplysningsforskriften. Prinsippet innebærer at det skal etableres tiltak for å sikre personopplysninger mot uautorisert eller utilsiktet tilgang, videregivelse, endring og/eller sletting, jf. Schartum og Bygrave 2011, s. 103.

[38] Jf. Rapport 2012 s. 71

[39] Jf. Rapport 2012 s. 65

[40] Når saken er aktiv, dvs. når den innsatte er registrert i Infoflyt-systemet.

[41] Jf. Rapport 2012 s. 66-68

[42] Jf. Rapport 2012 s. 66-68

[43] Med opplysningskvalitet menes her at de opplysningene som registreres er av en viss kvalitet, det vil si at de korrekte, at de er innhentet fra en pålitelig kilde, samt at det av de registrerte opplysningene fremkommer informasjon om hvem kilden er. Se også Schartum og Bygrave, 2011 s. 60-62

Mappene fremstod som lite oversiktlige da de ikke hadde dokumentliste og dokumentene lå uordnet i mappen.[44] I enkelte saker så det ut til at dokumenter manglet eller at korrespondansen hadde stoppet opp. Samt at det manglet system for oppdatering av opplysningene, f.eks. en plan for neste risikovurdering. Utvalget fant at mappenes innehold varierte fra sak til sak, og at det også forelå mye informasjon som ikke var sensitivt og som derfor kunne vært kommunisert i åpne kanaler. Funnene gav både eksempler på at innsatte var registrert i Infoflyt selv om trusselen ble ansett lavere enn i KSF 2/2005, og at innsatte ikke ble registrert i Infoflyt selv om de oppfylte kravene i rundskrivet. De vurderte sikkerhetsgraderingen til å være «noe tilfeldig».[45]

Infoflyt-utvalget fant også at det var vanskelig å finne ut hvem som hadde behandlet Infoflyt-saken og tatt beslutninger, eksempelvis om registreringen. Ved registrering i Infoflyt-systemet skal dette markeres med et flagg i Kompis-registeret[46]. Av funnene kom det imidlertid frem at det i enkelte saker ikke fremgikk av mappen når den innsatte ble flagget i Kompis[47], ei heller dokumentasjon på avflagging eller saksbehandling tilknyttet vurderingen av om en registrert burde ut av systemet. Det manglet også ofte en begrunnelse for flaggingen/avflaggingen.[48]

Infoflyt-utvalgets funn viser at det er behov for et enhetlig regelverk som er tilpasset Infoflyt-systemet, samt at den innsattes behov for innsyn i lagrede personopplysningene er berettiget. Nedenfor redegjøres det for hvordan Infoflyt er regulert etter gjeldende rett.

[44] Jf. Rapport 2012 s. 66-68

[45] Jf. Rapport 2012 s. 66-68

[46] Kompis er et elektronisk register som brukes til å registrere ordinær fangeinformasjon som hendelsesrapporter, fangejournaler osv. jf. Rapport 2012 s. 42. Ved registrering i Infoflyt-systemet markeres dette med et flagg i kompis. Flagget indikerer at det skal innhentes informasjon fra KDI før det eventuelt fattes vedtak i saken.

[47] Dato fremgikk imidlertid i Kompis

[48] Jf. Rapport 2012 s. 66-68

2.3 Kort redegjørelse for regulering av Infoflyt-systemet etter gjeldende rett

2.3.1 Innledning

Denne delen er ment å gi en kort innføring i hva Infoflyt-systemet er, hvem som kan registreres der og hvordan registreringen foregår. Dette redegjøres det for i pkt. 2.3.2 og 2.3.3. For å gi et sammenligningsgrunnlag til lovforslaget, redegjøres det også kort for rettsgrunnlaget etter gjeldende rett i pkt. 2.3.4 og 2.3.5. Selve sammenligningen mellom gjeldende rett og lovforslaget fremgår hovedsakelig i pkt. 3.6 og 4.4.

2.3.2 Formål og vilkår for registrering etter gjeldende rett

Formålet med instruks KSF 2/2005 er å bedre informasjonssamarbeidet mellom kriminalomsorgen og politiet i «særlige alvorlige saker og med særlig høy risiko».[49] Videre er Infoflyt-systemet ment å sikre kriminalomsorgen et så godt informasjonsgrunnlag som mulig, slik at det kan foretas «riktige sikkerhetsmessige vurderinger», både for løpende vurderinger ved den enkelte enhet, men også ved nyinnsettelser, soningsoverføringer og i trusselsaker.[50]

Målgruppen for Infoflyt-systemet er «(…) personer som etter en konkret vurdering av de ulike faktorer utgjør en særlig risiko for orden og sikkerhet i fengselet, for tjenestemennene der og for samfunnet for øvrig.» [51] Etter KSF 2/2005 omfatter dette innsatte og domfelte som antas å medføre særlig rømningsfare, fare for anslag utenfra for å bistå til rømning, gisseltaking, fare for ny særlig alvorlig kriminalitet, samt innsatte som har et spesielt beskyttelsesbehov, og personer som er tilknyttet et organisert kriminelt nettverk. [52] Med i helhetsvurderingen for registreringen tas hensyn til type lovbrudd, domslengde og tidligere adferd i fengselet, for eksempel nye alvorlige straffbare forhold. I tillegg kan tilhørighet til organiserte kriminelle

[49] Jf. KSF 2/2005 s. 1
[50] Jf. KSF 2/2005 s. 1
[51] Jf. KSF 2/2005 s. 2
[52] Jf. KSF 2/2005 s. 2

nettverk, politiske- eller religiøse ekstreme nettverk medføre registrering. Videre kan også tredjepersoner i kontakt med den registrerte bli registrert.[53]

2.3.3 Registreringen

Det er KDI som avgjør om en innsatt skal registreres i Infoflyt-systemet.[54] Selve informasjonsutvekslingen mellom kriminalomsorgen og politiet foregår og kvalitetssikres på sentralt nivå mellom KDI og Kripos, eller eventuelt mellom KDI og PST.[55] For opplysninger som er innhentet av kriminalomsorgen er det KDI, som ut fra art og alvorlighetsgrad, vurderer om opplysningene skal registreres i Infoflyt.[56] Det at registreringen er merket med flagg i Kompis signaliserer at overordnet nivå må kontaktes før det fattes vedtak lokalt i fengselet. [57]

Etter KSF 2/2005 er det aktuelt å registrere opplysninger som fremkomme av politiets etterforskning eller under den registrertes soning, eksempelvis bearbeidete opplysninger fra Kompis, informasjon fra andre innsatte, informasjon fra tredjepersoner, brev-, telefon- og besøkskontroll samt andre observasjoner fra ansatte i kriminalomsorgen.[58] I tillegg til disse opplysningene kan det være aktuelt å registrere opplysninger om hvilket sikkerhetsnivå den innsatte soner ved, andre innsatte som soner ved samme avdeling, reaksjoner på brudd, soningsoverføringer, permisjoner, og besøkstillatelser.

2.3.4 Kort om retten til informasjon og innsyn etter personopplysningsloven

Som vist under redegjørelsen av Infoflyt-utvalgets funn i pkt. 2.2.1 kom utvalget til at strgjfl. kapittel 1a ikke gav tilstrekkelig klart hjemmelsgrunnlag for Infoflyt-systemet. Etter dette kom utvalget til at Infoflyt-systemet, frem til nytt hjemmelsgrunnlag forelå, måtte reguleres

[53] Jf. KSF 2/2005 s. 2

[54] At det er KDI som har kompetanse til å bestemme hvem som skal registreres i Infoflyt-systemet står ikke eksplisitt i KSF 2/2005, men følger av sammenhengen i instruksen, da det eksempelvis er KDI som er behandlingsansvarlig, og da det er KDI som vurderer om en opplysning skal registreres i Infoflyt eller ikke.

[55] Jf. KSF 2/2005 s. 3, se også Rapport 2012 s. 41

[56] Jf. KSF 2/2005 s. 3, se også Rapport 2012 s. 44

[57] Jf. KSF 2/2005 s. 4

[58] Jf. KSF 2/2005 s. 2

etter personopplysningsloven.[59] Nedenfor følger derfor en kort redegjørelse av for personopplysningslovens regler om innsynsrett.

Retten til *informasjon* ved behandling av personopplysninger reguleres i popplyl. § 19. Når det samles inn opplysninger fra den registrerte, har den behandlingsansvarlige[60] plikt til å informere den registrerte om at dette skjer, formålet med behandlingen, om opplysningene vil bli utlevert og eventuelt til hvem, samt opplysninger som gjør den registrerte i stand til å ivareta sine andre rettigheter som retting og sletting etter §§ 27 og 28.[61] Det kan imidlertid gjøres unntak fra informasjonsplikten i medhold av den generelle unntaksbestemmelsen i popplyl. § 23 som gjennomgås nedenfor.

Retten til *innsyn* reguleres etter popplyl. § 18. Bestemmelsen skiller mellom generell og spesiell innsynsrett, jf. henholdsvis første og annet ledd. Enhver har rett til å be om innsyn i de behandlinger som foretas av den behandlingsansvarlige, og det følger ytterligere rettigheter etter annet ledd dersom man er registrert. Den registrerte kan etter tredje ledd be om at den behandlingsansvarlige utdyper informasjonen som gis, så langt det er nødvendig for at han skal kunne ivareta sine rettigheter, som f.eks. klage etter § 42. Innsyn kan gis muntlig, men den registrerte har krav på å få informasjonen skriftlig etter begjæring til den behandlingsansvarlige eller hans databehandler[62], jf. § 24. I likhet med unntak fra informasjonsplikten nevnt over, kan det også gjøres unntak fra innsynsretten etter popplyl. § 23.

For Infoflyt-systemet vil alle disse bokstavene kunne være av relevans. De enkelte vilkår i bestemmelsen vil ikke bli utdypet her, da det er lovforslaget som særskilt skal vurderes i denne oppgaven. Som det vil fremgå av redegjørelsen i pkt. 3 er imidlertid flere av vilkårene i unntaksbestemmelsene like, og det vil bli knyttet merknader til dette.

---

[59] Det er imidlertid noe uklart om dette har blitt fulgt i praksis. I samtale med Kriminalomsorgens region øst ble jeg gjort oppmerksom på at deres praksis fulgte saksbehandlingsinstruksene i KSF 2/2005 som viser til strgjfl. § 7 bokstav c.

[60] Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger, og hvilke hjelpemidler som skal benyttes, jf. popplyl. § 2 nr. 2.

[61] Jf. Popplyl. § 19 bokstavene a, b, c og e

[62] Databehandler vil si den som behandler personopplysninger på vegne av behandlingsansvarlige, jf. popplyl. § 2 nr. 5.

Unntaksbestemmelsen i popplyl. § 23 (1) bokstavene a til f oppstiller en rekke alternative vilkår for når det kan gjøres unntak fra informasjonsplikt og innsynsrett. For Infoflyt-systemet er det særlig bokstavene a og b som er aktuelle. Bokstav a omhandler hensyn til «rikets sikkerhet, landets forsvar», «forholdet til fremmede makter» og «internasjonale organisasjoner», og bokstav b angår hensyn til «forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger». Da disse vilkårene også er representert i lovforslaget, vil tolkningen av vilkårene foretas under del 3. Ved innsynsnekt har den registrerte krav på å få skriftlig begrunnelse, med presis henvisning til unntakshjemmelen, jf. § 23 (3).

2.3.5 Kort om den registrertes klage- og kontrollmuligheter

Dersom den registrerte får avslag på sin innsynsbegjæring, kan han klage til overordnet organ, jf. fvl. § 28 jf. strgjfl. § 7. Er vedtaket fattet på regionalt nivå etter strgjfl. § 6(2), er det KDI som er overordnet organ. Det er Justis- og beredskapsdepartementet som eventuelt behandler klage over vedtak fattet av KDI. Den registrerte kan føre sak om innsynsnekt for domstolen etter tvistelovens regler.[63]

Datatilsynet har tilsynsmyndighet med kriminalomsorgens behandling av personopplysninger, herunder Infoflyt-systemet, jf. popplyl. § 42. Datatilsynet kan gi pålegg om opphør eller atferdsendring og kan ilegge sanksjoner som tvangsmulkt, overtredelsesgebyr og anmelde til politiet, jf. popplyl. § 48.[64] Tilsynet har også kompetanse til å tilkjenne erstatning etter popplyl. § 49. Sivilombudsmannen fører kontroll med forvaltningen, jf. ombudsmannsloven § 4, og kan ta saker til behandling etter klage fra den registrerte eller av eget tiltak, jf. ombudsmannsloven § 5. Ombudsmannen avgjør om en sak tas til behandling, jf. § 6 (4). Uttalelsene fra Sivilombudsmannen er ikke bindende, jf. § 10, men blir tradisjonelt fulgt av forvaltningen.

[63] Tvisteloven, lov av 17.6.2005 nr. 90

[64] Se Rapport. 2012 s. 32

3 Reglene om innsyn jf. Prop. 120 L (2013-2014)

3.1 Innledning

I denne delen redegjøres det for innsynsretten etter lovforslaget. Pkt. 3.4 tar for seg utgangspunktet for innsynsrett, mens pkt. 3.5 tar for seg unntakene. Hvert punkt oppsummeres avslutningsvis. I pkt. 3.6 oppsummeres innsynsbestemmelsen for så å vurderes opp mot gjeldende rett.

Ettersom det er en forutsetning for å kunne kreve innsyn at man kjenner til registreringen, gis det også en kort redegjørelse for informasjonsplikten i pkt. 3.3. Aller først redegjøres det imidlertid for hensyn som taler for og mot innsyn i pkt. 3.2.

3.2 Hensyn som taler for og mot innsyn

Innsynsretten er viktig for den registrerte av minst to årsaker. For det første vil han ha interesse av innsyn dersom det er fattet et vedtak i hans disfavør begrunnet med opplysninger som er registrert i Infoflyt uten at disse fremgår. For å kunne imøtegå disse opplysningene og forsvare seg, vil han være avhengig av å vite hva disse opplysningene går ut på. Hvis opplysningene er gamle eller ukorrekte, vil han ha behov for å korrigere disse.

For det andre vil han ha interesse av å få innsyn for å verne om sine personopplysninger. Det vil kunne være av viktighet for den innsatte å vite hva slags opplysninger som behandles, og hvordan disse behandles. Eksempelvis vil det være kunne være av betydning hvor mange som har tilgang på opplysningene, og hvordan rutinene er for oppbevaring av opplysningene og eventuell spredning av disse.

Ved å forenkle informasjonsflyten mellom kriminalomsorgen og politiet, får kriminalomsorgen et bedre grunnlag for å foreta sviktfarevurderingen[65] og andre risikovurderinger som igjen

[65] Sviktfarevurdering: Den vurderingen som foretas før utgang av fengsel, eksempelvis ved permisjon eller prøveløslatelse, jf. Storvik, 2011 s. 256. Utgang skal nektes dersom det er «grunn til å anta» at den innsatte begår nye straffbare handlinger, unndrar seg straffegjennomføring, eller ikke følger de vilkår som er fastsatt for utgang av fengsel. (ibid) Sviktfarevurderingen fremgår av strgjfl. §§ 2 og 3.

kan føre til målrettede tiltak. Politiet kan få verdifull informasjon som setter dem i stand til å foreta politioppgaver, som videre etterforskning, sikkerhetstiltak for å forhindre planlagte kriminelle aksjoner, sikkerhetstiltak rundt nøkkelpersoner som vitner eller kriminelle mål mv. I tillegg til det ovennevnte muliggjør Infoflyt-systemet sammenstilling av opplysninger, slik at en kan avdekke mønstre eller se utviklingstrekk, som igjen kan føre til at hendelser eller tendenser kan oppdages og forhindres tidligere.

Å gi innsyn i opplysningene kan for det første avdekke kriminalomsorgens og politiets metoder for innsamling av informasjon, men det kan også gi informasjon om hvilke opplysninger forvaltningen har kontra hva forvaltningen ikke har. I kriminalomsorgen kan det være problematisk å gi innsyn fordi det kan gjøre arbeidet i fengselet vanskeligere. Eksempelvis kan innsyn vise hvem det er som har registrert opplysningene, som igjen kan gjøre relasjonen mellom innsatt og betjent vanskelig. Videre kan det utgjøre en fare for sikkerheten i fengselet dersom det fremkommer opplysninger om rutiner i anstalten. Det kan vanskeliggjøre kriminalomsorgen og politiets arbeid å gi innsyn, fordi den registrerte da kan endre eller tilpasse sin adferd etter hva som har kommet frem av opplysninger. Videre kan det utgjøre en fare for andre personer dersom opplysninger blir kjent, for eksempel personer i vitne program eller den domfeltes nærstående. Det vil for eksempel kunne innebære fare for liv og helse til en innsatt, dersom det blir kjent for andre innsatte at han er vitne i en pågående rettssak.

3.3 Forutsetning for effektiv innsynsrett, kort om informasjonsplikten

Det er en forutsetning for å kunne be om innsyn eller kontroll av sine registrerte opplysninger, at den innsatte kjenner til at det finnes et Infoflyt-system og at han er registrert der. Informasjonsplikten underbygger således både innsynsretten og adgangen til å få sine opplysninger kontrollert. Informasjonsplikten er foreslått regulert i strgjfl. § 4g som lyder som følger:

> «§ 4 g Kriminalomsorgens informasjonsplikt
>
> Den behandlingsansvarlige i kriminalomsorgen skal informere den registrerte om at det behandles personopplysninger om vedkommende i Infoflyt-systemet og at opplysningene kan utleveres til politiet og påtalemyndigheten etter § 4 i.
>
> Den behandlingsansvarlige kan unnlate å informere den registrerte dersom
>
> a) det er nødvendig for å ivareta formålene i § 4 f første ledd bokstav a til e

b) det er nødvendig av hensyn til nasjonal eller offentlig sikkerhet

c) opplysningene er mottatt fra Politiets sikkerhetstjeneste

d) den registrerte ikke er innsatt eller domfelt og det ikke opprettes en egen sak på vedkommende i Infoflyt-systemet.»

Utgangspunktet etter § 4g er at kriminalomsorgen av eget tiltak[66] skal gi den registrerte informasjon om at han er registrert, samt at utlevering av informasjon til politi- og påtalemyndighet kan forekomme. Det skal også gis informasjon om andre rettigheter knyttet til registreringen, som innsyn, sletting og klagerett, samt reglene om å be Datatilsynet om kontroll.[67] Informasjonsplikten omhandler ikke de konkrete opplysningene som er registrert, da dette reguleres av innsynsregelen, jf. § 4h.

Departementet uttaler om informasjonsplikten at det er større nødvendighet for å unnta informasjonsplikten i politiet enn i kriminalomsorgen, og at utgangspunktet derfor bør være at den registrerte skal gis informasjon om behandling av personopplysninger i Infoflyt-systemet når det opprettes sak.[68] Dette utdypes ikke nærmere, men det er tenkelig at årsaken er at politiet i større grad enn kriminalomsorgen er et kriminaltetsforbyggende og -bekjempende organ, og at slik informasjon eksempelvis kan være ødeleggende for etterforskning. Det er imidlertid også anledning til å unnta informasjonsplikten i kriminalomsorgen. I bestemmelsens annet ledd følger flere alternative vilkår. Med unntak av bokstav d, [69] er unntakene identiske med unntakene i innsynsrettbestemmelsen. Redegjørelsen for unntakene foretas i neste punkt om innsynsrett.

Vurderingen av hvorvidt registreringen skal unntas informasjonsplikten av hensyn til sikkerhet skal gjøres konkret i det enkelte tilfellet.[70] I følge lovforslaget er begrunnelsen for at det kan gjøres unntak fra informasjonsplikten at det finnes tilfeller der slik informasjon kan medføre fare for andre personer, samfunnets sikkerhet eller offentlig orden. Departementet frem-

[66] Jf. departementets vurdering, Prop. 120L (2013-2014) s. 26

[67] Jf. merknad til bestemmelsen, Prop. 120L (2013-2014) s. 31-32

[68] Jf. Prop. 120 L (2013-2014) s. 26

[69] Bokstav d angår registrerte som ikke er domfelt. Denne gruppen faller således utenfor problemstillingen, og bokstav d redegjøres derfor ikke her.

[70] Jf. Prop. 120 L (2013-2014) s. 26

hever at hensynet til samfunnets sikkerhet må veie tyngre enn hensynet til den registrertes personvern for at det skal kunne gjøres unntak.[71] Det vil bli redegjort nærmere for dette i redegjørelsen for innsynsrett under neste punkt.

3.4 Hva innebærer retten til å be om innsyn og hvem gjelder den for?

Innsynsrett er en forutsetning for kontradiksjon og ivaretakelse av eget personvern. Innsynsretten forslås regulert i strgjfl. § 4h, og utgangspunktet følger av første ledd:

> «Den registrerte som ber om det, skal gis innsyn i de opplysningene som er registrert om vedkommende i Infoflyt-systemet og de opplysningene som er utlevert til politiet og påtalemyndigheten.»

Utgangspunktet er at en registrert som begjærer innsynrett skal få det, og at retten er begrenset til å kun gjelde personopplysninger om han selv. Ordlyden innebærer at den som ikke begjærer innsyn, ikke får vite hva som er registeret.

I merknad til innsynsbestemmelsen fremgår det at begjæring skal fremsettes for behandlingsansvarlig.[72] Hva behandlingsansvaret innebærer og hvem som er behandlingsansvarlig foreslås regulert i forskrift i forslaget, jf. § 4k bokstav a. Etter strgjfl. § 4b er behandlingsansvarlig den som etter lov eller forskrift bestemmer formålet med behandling av personopplysninger og hvilke hjelpemidler som skal brukes.[73] Videre har behandlingsansvarlig ansvaret for at alle regulatoriske krav til behandlingen er oppfylt, og det er hit den registrerte kan henvende seg for å gjøre sine rettigheter gjeldende.[74]

Innsynsretten gjelder både samlede opplysninger og utleverte opplysninger i § 4h (1). Samlede opplysninger vil si opplysninger som kriminalomsorgen har registrert og som politiet og påtalemyndighet har levert til kriminalomsorgen, mens det med utleverte opplysninger menes opplysninger som kriminalomsorgen har utlevert til politiet. Ordlyden i første ledd omfatter

[71] Jf. Prop. 120 L (2013-2014) s. 26
[72] Jf. Prop. 120 L (2013-2014) s. 32
[73] Se også popplyl. § 2 nr. 4
[74] Jf. Rapport 2012 s. 28

ikke begrensninger som tilsier at det skal vurderes delvis innsyn. Da delvis innsyn reguleres nærmere i annet ledd, må det kunne antas at utgangspunktet er at det skal gis fullt innsyn.

Etter første ledd er altså utgangspunktet at den registrerte kan be om innsyn i opplysninger registrert om seg selv, at han skal få fullt innsyn og at innsynet også skal omfatte informasjon om eventuell utlevering av opplysningene.

3.5 Redegjørelse av unntakene fra innsynsrett

3.5.1 Unntak for innsynsrett for å ivareta formålene med behandling av personopplysninger i Infoflyt-systemet

Fra utgangspunktet om innsynsrett kan det gjøres unntak, dersom det anses nødvendig for å ivareta formålene i strgjfl. § 4f (1) bokstavene a til e.[75] Det skal etter denne bestemmelse vurderes om innsyn kan gis delvis eller om det må fattes vedtak om innsynsnekt. I merknad til bestemmelsen fremgår det at delvis innsyn skal gis dersom formålene kan ivaretas.[76]

Unntaket er bygget opp slik at dersom en person er kvalifisert for registrering i Infoflyt-systemet etter § 4f, så er han også i utgangspunktet kvalifisert for å unntas innsynsretten. Det stilles imidlertid krav om at innsynsnekt etter en vurdering fremstår som nødvendig for å ivareta formålene i § 4f (1) bokstavene a til f. Fordi dette unntaket tar opp i seg formålsbestemmelsen, samt krever en nærmere redegjørelse av nødvendighetsvilkåret, vil redegjørelsen deles opp i underpunkter for å gjøre det mer oversiktlig. Redegjørelsen for formålene følger i pkt. 3.5.1.1 og nødvendighetsvurderingen i pkt. 3.5.1.2. I pkt. 3.5.1.3 følger en oppsummering av unntaket.

[75] Ordlyden i unntaksbestemmelsen § 4h (2) bokstav a: «Innsyn kan nektes helt eller delvis dersom a) det er nødvendig for å ivareta formålene i § 4f (1) bokstav a til e»

[76] Jf. Prop. 120L (2013-2014) s. 32

3.5.1.1 Redegjørelse for formålene

Hovedformålet med Infoflyt-systemet er å forebygge, forhindre og bekjempe særlig alvorlig kriminalitet, jf. § 4f (1). Ettersom formålene utgjør vilkår i unntaksbestemmelsen i strgjfl. § 4h (2), vil de i redegjørelsen nedenfor omtales som vilkår.

> «§ 4f Formålet med behandlingen av personopplysninger i Infoflyt-systemet
>
> Kriminalomsorgen kan behandle personopplysninger om domfelte og innsatte i Infoflytsystemet dersom det er nødvendig for å
>
> a) forebygge og forhindre rømning når det foreligger rømningsfare
>
> b) forebygge og forhindre anslag utenfra for å bistå til rømning
>
> c) forebygge og forhindre gisseltaking
>
> d) forebygge, forhindre og bekjempe organisert kriminalitet, terror, voldelig ekstremisme eller annen alvorlig kriminalitet under gjennomføringen av varetekt, straff og andre strafferettslige reaksjoner eller
>
> e) ivareta sikkerheten til innsatte eller domfelte eller andre personer med spesielt beskyttelsesbehov.»[77]

«Forebygge» er et vilkår i bokstavene a til d, og står sammen med vilkåret «forhindre». En naturlig språklig forståelse av ordet «forebygge» er tiltak som iverksettes i forkant av en forutsett hendelse for å motvirke eller avverge at den inntreffer. Formålet «forebygge kriminalitet» kan minne om vilkåret «motvirke nye straffbare handlinger» i formålsbestemmelsen til straffegjennomføringsloven, jf. § 2. Det fremkommer av forarbeidene til straffegjennomføringsloven at å motvirke ny kriminalitet er et viktig overordnet hensyn for kriminalomsorgens straffegjennomføring.[78] Dette ivaretas ved at den domfelte i stor grad er isolert fra samfunnet, ved sikkerhetsvurderinger i forkant av permisjon e.l., i tillegg til at straffen søkes å virke rehabiliterende.[79] Infoflyt-systemet er et verktøy som kan benyttes i forebyggingsarbeidet for å opprettholde sikkerheten i fengselet, samt å bidra til politiets arbeid i å forebygge kriminelle handlinger.

---

[77] Jf. strgjfl. § 4f (1)

[78] Jf. Ot.prp. nr.5 (2000-2001) Om lov om gjennomføring av straff mv. (straffegjennomføringsloven) pkt. 13

[79] Jf. Storvik, 2011 s. 35

«Forhindre» er et vilkår i bokstavene a til d, og står sammen med vilkåret «forebygge». *Forhindre* innebærer at man iverksetter et tiltak for at antatt utfall ikke skal inntreffe. Begrepet kan minne om *avverge*, som blant annet benyttes i politiregisterloven. På grunn av Infoflyt-systemets rolle mellom kriminalomsorgen og politiet, var politiregisterloven viktig under arbeidet med Infoflyt-utvalgets lovutkast. Deres lovutkast innebar blant annet en rekke henvisninger til politiregisterloven. Hovedgrunnen til at en henvisningsløsning ble valgt bort av departementet, var av praktiske hensyn for saksbehandlerne i kriminalomsorgen. Politiregisterlovens begrep kan likevel belyse betydningen av ordet forhindre. Etter polregl. § 27 (1) kan det gjøres unntak fra taushetsplikten dersom det vil være nødvendig for å *avverge* en straffbar handling. Avverge brukes i denne sammenheng i motsetning til å forebygge i annet ledd. Vilkåret avverge krever både at det foreligger forholdsvis konkret og troverdig informasjon om at en kriminell handling vil bli begått, og at utførelsen er forholdsvis nært i tid.[80] Både tekstsammenheng og begrepsbruk taler for en lik forståelse av begrepene i lovforslaget. Etter dette har jeg kommet til at *forhindre* må tolkes slik politiregisterloven benytter vilkåret *avverge*, og vil således kreve at det foreligger forholdsvis konkret og troverdig informasjon om at en kriminell handling vil bli begått. Da vilkårene «forebygge og forhindre» står bundet sammen taler dette for at begge vilkårene må være oppfylt for at Infoflyt-systemet skal kunne benyttes.

Vilkåret «bekjempe» er kun nevnt i bokstav d, og står sammen med vilkårene «forebygge» og «forhindre». En naturlig språklig forståelse av ordet *bekjempe* kan i denne sammenheng innebære at det skal kjempes mot, tas opp en kamp mot og motarbeide kriminalitet. Bekjempe kriminalitet har tradisjonelt sett ikke vært en oppgave for kriminalomsorgen, og ordet er heller ikke benyttet andre steder i straffegjennomføringsloven, men er ikke nytt i Infoflyt-sammenheng, jf. KSF 2/2005. Departementet understreker at det er politiet som skal bekjempe kriminalitet, men at kriminalomsorgen også har en viktig rolle i så måte, fordi den skal foreta sikkerhetsvurderinger, arbeide mot at den innsatte foretar kriminelle handlinger pånytt, både før og etter endt soning.[81] Dette er oppgaver som tradisjonelt har tilligget kriminalomsorgen, selv om ordet «bekjempe» ikke i særlig grad er benyttet tidligere. «Bekjempe» står ikke alene, men sammenbundet med vilkårene «forebygge» og «forhindre». Dette kan kan tyde på at det kreves noe mer enn kun å forebygge og forhindre, for at denne bokstaven skal

[80] Jf. Ot.prp. nr. 108 (2008-2009) Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) pkt. 21.6

[81] Jf. Prop. 120 L (2013-2014) s. 18

kunne benyttes som grunnlag for å ta i bruk Infoflyt-systemet. «Bekjempe» tar på et vis opp i seg både det å forebygge og å forhindre en handling, men kan kanskje synes noe mer aktivt og målrettet enn disse begrepene. Ser man vilkåret i sammenheng med de alvorlige handlingene som skal bekjempes («organisert kriminalitet, terror, voldelig ekstremisme eller annen alvorlig kriminalitet»[82]), er disse nokså ekstreme og kan potensielt utgjøre en større fare enn kriminaliteten som det vises til i de andre bokstavene (henholdsvis «rømning»[83], «gisseltaking»[84] eller «ivareta sikkerheten til innsatte eller domfelte eller andre personer med spesielt beskyttelsesbehov»[85]). De kriminelle handlingene som skal bekjempes gir således en indikator på hvilket alvor som må foreligge for at en kan si at en skal bekjempe noe, samtidig som vilkåret bekjempe tilsier at de oppramsede kriminelle handlingene har en viss prioritet.

Fra redegjørelsen over om formålene forebygge, forhindre og bekjempe kriminalitet, kan en trekke ut at formålet om å forebygge kriminalitet vil være tilstede under hele straffegjennomføringen, mens formålet forhindre kriminalitet kun vil være tilstede når faren er mer konkret og nært forestående i tid. Formålet om å bekjempe kriminalitet er nærmere knyttet til bestemte alvorlige former for kriminalitet, som det det vil være nærliggende å prioritere arbeid mot. Formålene vil således favne om hele soningsforløpet til den domfelte, men vil ikke nødvendigvis være like fremtredende under hele soningen. Dette vil ha betydning i vurderingen av om det skal gis innsynsnekt eller om innsyn kun skal unntas delvis. I merknad til bestemmelsen fremgår det at delvis innsyn skal gis dersom formålene kan ivaretas.[86]

3.5.1.2 Er det nødvendig å nekte innsyn?

Ordlyden i både § 4h (2) bokstav a og b legger eksplisitt opp til at det skal foretas en vurdering av om det kan være *nødvendig* å unnta innsynsretten. Det er ikke gitt merknader til bestemmelsen i forslaget for hvordan nødvendighetsvurderingen skal foretas, men da Infoflyt-systemet utgjør et inngrep i personvernet jf. EMK art. 8[87], vil nødvendighetsvurderingen slik

[82] Jf. strgjfl. § 4f(1) bokstav d
[83] Jf. strgjfl. § 4f (1) bokstav a og b
[84] Jf. strgjfl. § 4f (1) bokstav c
[85] Jf. strgjfl. § 4f (1) bokstav e
[86] Jf. Prop. 120L (2013-2014) s. 32
[87] Se bl.a. avgjørelsene Leander mot Sverige saksnr. 9248/81 og Peck mot Storbritannia saksnr. 44647/98

den praktiseres av EMD kunne være førende for den vurderingen som må gjøres i strgjfl. § 4h(2), jf. mfl. §§ 2 og 3.[88]

Utgangspunktet i EMK art. 8 (1) er at alle mennesker har rett til privatliv, herunder rett til personvern.[89] Rettigheten er imidlertid ikke absolutt, ettersom det kan gjøres inngrep i den etter annet ledd, forutsatt at det foreligger tre kumulative vilkår: inngrepet må ha hjemmel i lov, det må ha et relevant formål og inngrepet må være nødvendig i et demokratisk samfunn. Det forutsettes i den videre redegjørelsen at loven vil bli tilstrekkelig presis og tilgjengelig, [90] og slik forutberegnelig for det enkelte individ, [91] i tråd med EMDs praksis.

Artikkelen lister opp en rekke alternative hensyn som kan utgjøre et legitimt formål for et eventuelt inngrep, jf. EMK art. 8 (2). I lovforslaget trekker departementet frem at formålene som vil være relevante i denne sammenheng er hensynene til «nasjonal sikkerhet», «offentlig trygghet», «forebygging av uorden eller kriminalitet», «for å beskytte helse» eller «for å beskytte andres rettigheter og friheter».[92]

EMK art. 8 (2) stiller som nevnt krav om at inngrepet må være «nødvendig i et demokratisk samfunn». I Olsson mot Sverige presiseres nødvendighetskravet til å innebære et tvingende samfunnsbehov og at inngrepet er forholdsmessig i det konkrete tilfellet.[93] Det skal videre foretas en konkret helhetsvurdering[94]. I praksis blir de to elementene i nødvendighetsvurderingen ofte vurdert samlet.[95] Om det foreligger et tvingende samfunnsmessig behov vil bero på om inngrepet er egnet til å oppnå formålet.[96] Terskelen har vist seg å ligge et sted mellom ytterpunktene «uomgjengelig»[97] og «ønskelig» eller «nyttig».[98] For at inngrepet skal være

---

[88] Nødvendighet og forholdsmessighet er også et grunnleggende prinsipper i personvernretten, se eksempelvis personverndirektivet art. 6 (1) bokstav c, samt art. 7, 8 og 13.

[89] Jf. bl.a. Leander mot Sverige saknr. 9248/81

[90] Jf. Malone mot Storbritannia, saksnr. 8691/79

[91] Jf. Silver m.fl. mot Storbritannia, saksnr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75 §88

[92] Jf. Prop. 120 L (2013-2014) s. 17

[93] Jf. «Pressing social need and (…) proportionate to the legitime aim pursued», jf. Olsson mot Sverige. Se også Peck mot Storbritannia saksnr. 44646/98 § 76

[94] Jf. Peck mot Storbritannia saksnr. 44646/98 § 76

[95] Jf. Peck §§ 76-87

[96] Jf. «relevant and sufficient» Peck § 76, se Aall 2007 s 128

[97] «indispensable» Jf. Handyside mot Storbritannia saksnr. 5493/72 §§ 48-49 i Aall, 2007 s. 127

[98] Jf. Aall, 2007 s. 128-130

nødvendig må det også vise seg å være forholdsmessighet mellom det målet en ønsker å oppnå, og det middelet eller inngrepet som benyttes for å nå dette målet. Inngrepets styrke mot den som rammes og hans interesser må veies mot de hensyn som tilsier inngrepet. Intensitet i forholdsmessighetsvurderingen vil variere med inngrepets styrke.[99] Det skal altså foretas en interesseavveining mellom motsetningene i saken, men det må også tas hensyn til hvordan den enkelte berøres av inngrepet (inngrepet styrke). Inngrep i privatlivet har tradisjonelt vært ansett som et stort inngrep.[100]

For at det skal kunne fattes vedtak om innsynsnekt må det etter dette vises at innsynsnekt vil være egnet til å oppnå formålene i § 4f (1) bokstavene a til e, og det må vurderes om delvis innsyn vil være tilstrekkelig for å ivareta formålene.

Av forarbeidene fremgår det at det i helhetsvurderingen særlig skal legges vekt på «forhold som kan medføre fare for at tiltak for å ivareta formål med registeringen blir avslørt og dermed ineffektive.»[101] Om slik fare foreligger vil blant annet kunne avhenge av hvor konkret faren er og hvor nært faren kan inntreffe i tid. Som det ble vist under redegjørelsen ovenfor, så vil formålene i prinsippet kunne favne om hele soningsforløpet til den domfelte. De vil imidlertid ikke nødvendigvis være like fremtredende under hele soningen. Vurderingen av om det er nødvendig å unnta innsyn eller om det skal gis delvis innsyn vil således kunne bero på alvorlighetsgraden i situasjonen. I merknad til bestemmelsen fremgår det at delvis innsyn skal gis dersom formålene kan ivaretas.[102] Foreligger det for eksempel opplysninger som kan sette et vitnes liv i fare, vil det antakelig være anledning til å gi innsynsnekt for dette dokumentet i forkant av og under hovedforhandlingene i en rettssak, mens det etter rettssaken vil være uproblematisk å gi innsyn fordi opplysningene allerede er kjent.

Videre skal det vurderes om det er forholdsmessig å ikke gi innsyn i opplysningene som er registrert om vedkommende, satt opp mot den betydningen dette har for den registrerte. For kriminalomsorgen vil det kunne ha sikkerhetsmessig betydning dersom opplysninger blir kjent, men som det fremgår over vil ikke dette behovet nødvendigvis være like stort til enhver

[99] Jf. Aall, 2007 s. 128-130
[100] Jf. Dudgeon mot Storbritannia 22.10.1981 i Aall, 2007 s. 100
[101] Jf. Prop. 120 L (2013-2014) s. 32
[102] Jf. Prop. 120L (2013-2014) s. 32

tid. I forholdsmessighetsvurderingen vil det slik sett kunne ha betydning *hvilket* formål som skal beskyttes. Man kan tenke seg at det for eksempel vil kunne være forskjell på om det foreligger rømningsfare eller om det står om livet til en ansatt. Alvorlighetsgraden vil altså være et moment. Kriminalomsorgens behov må veies opp mot den registrertes behov for å få innsyn. Behovet til den registrerte vil også kunne variere gjennom soningen. Dersom den domfelte vet at han er registrert i Infoflyt-systemet vil han nok ha et behov for å vite hva som er registrert om han, uavhengig av andre forhold, fordi systemet innebærer at det samles inn store mengder personlige opplysninger. Behovet vil likevel antakelig være større dersom det foreligger negative vedtak eller foreligger indisier på at opplysningene ikke er korrekte, fordi han da vil ha et behov for å imøtegå de påstander som danner grunnlag for vedtaket, samt rette opplysninger som eventuelt er feilregistrert.

3.5.1.3 Oppsummering og konklusjon

Som nevnt er unntaket bygget opp slik at dersom en person er kvalifisert for registrering i Infoflyt-systemet etter strgjfl. § 4f, så er han også i utgangspunktet kvalifisert for å unnta innsynsretten. Kravet til at det skal foretas en nødvendighetsvurdering tilsier imidlertid at det skal foretas en konkret vurdering der det tas hensyn til om innsynsnekt vil være egnet til å oppnå formålet og om det vil være forholdsmessig.

3.5.2 Unntak for innsynsrett for å ivareta nasjonal og offentlig sikkerhet

Det kan gjøres unntak fra utgangspunktet om innsynsrett etter § 4h (1) bokstav b, dersom det vurderes nødvendig av hensyn til nasjonal eller offentlig sikkerhet.[103] Som etter unntaket i § 4h (2) bokstav a, skal det vurderes om det kan gis delvis innsyn, eller om det må fattes vedtak om innsynsnekt. Videre skal det gjennomgås en nødvendighetsvurdering slik det er redegjort for under pkt. 3.5.1.2.

Det foreligger ikke merknader til bestemmelsen i forslaget. Vilkåret «nasjonal sikkerhet» benyttes i ulike sammenhenger flere steder i lovgivningen, uten at det er tydelig redegjort for hva begrepet innebærer. Vilkårene nasjonal og offentlig sikkerhet, vil bli gjennomgått hen-

[103] «Innsyn kan nektes helt eller delvis dersom b) det er nødvendig av hensyn til nasjonal eller offentlig sikkerhet», jf. strgjfl. § 4h (1) bokstav b.

holdsvis i pkt. 3.5.2.1 og 3.5.2.2, før de sammenstilles og anvendes i drøftelsen av forslaget i pkt. 3.5.2.3.

3.5.2.1 Redegjørelse for vilkåret «nasjonal sikkerhet»

Vilkåret «av hensyn til nasjonal sikkerhet» benyttes i forvaltningsloven § 19(1) bokstav a, som regulerer unntak fra innsynsrett i forvaltningen. For tolkning av vilkåret vises det i bestemmelsene til offentleglova (offl.) §§ 20 og 21. Offentleglova regulerer innsyn i dokumenter i offentlig virksomhet. Bestemmelsene erstatter den tidligere offentlighetsloven § 6 (1) som gav åpning for å unnta et offentlighet dokument som dersom det ble kjent «kunne skade rikets sikkerhet». Etter dagens offl. § 21 kan det gjøres unntak fra innsynsrett «når det er påkravd av nasjonale tryggingsomsyn eller forsvaret av landet». Offentleglova § 21 bygger på forslag til loven fra NOU 2003:30[104] s. 297 og 278, der formuleringen «rikets sikkerhet» ble benyttet. Det kommer frem av forarbeidene til offentleglova at endringen i ordlyden, fra rikets sikkerhet til nasjonale sikkerhetshensyn, kun ble gjort av lovtekniske hensyn og at dette ikke var ment å utgjøre noen realitetsforskjell.[105] Hensynet til nasjonal sikkerhet vil for eksempel verne om opplysninger som kan skade virksomheten til politiet, herunder sikkerhetspolitiet, og det sivile beredskapsopplegget i samfunnet.[106] Det er hevdet i *Kommentarer til offentleglova* at offl. § 21, ut fra overskrift og sammenheng, antakelig avgrenser mot mer «sivile» sikkerhetshensyn, da dette ansees uttømmende regulert av offl. § 24.[107]

Begrepet «rikets sikkerhet» brukes i utlendingsloven og enkelte andre lover.[108] Begrepet er dynamisk og gis betydning ut fra den sammenheng det inngår i.[109] Det antas for eksempel i forarbeidene til loven at det får en snevrere rekkevidde i strafferettslig sammenheng enn den har etter utlendingsloven. I utlendingsloven har vilkåret «rikets sikkerhet» flere steder blitt erstattet med «grunnleggende nasjonale interesser», som i forarbeidene er uttalt som mer i takt

[104] NOU 2003:30 Ny offentlighetslov

[105] Ot.prp. nr. 102 (2004-2005) Om lov om rett til innsyn i dokument i offentleg verksemd (offentleglova) s. 143

[106] Ot.prp. nr. 102 (2004-2005) s. 143

[107] Jf. Bernt, 2014.

[108] Se f.eks. straffeloven, lov av 22.5.1905 nr. 10 og sikkerhetsloven, lov av 20.3.1981 nr. 25

[109] Jf. Ot.prp. nr. 75 (2006-2007) Om lov om utlendingers adgang til riket og deres opphold her (utlendingsloven) pkt. 18.1.1.

med senere tids utvikling av trusselbildet.[110] Denne tendensen er kommentert i Rt. 2007 s.1573 der Høyesterett vurderte gyldigheten av Utlendingsnemndas vedtak etter utl. § 30 (2) bokstav a, og der utvisning ble ansett nødvendig av hensyn til rikets sikkerhet. Høyesterett bemerket i premiss 55 at heller ikke begrepet «rikets sikkerhet» er av statisk karakter. Fra det som ovenfor er nevnt kan det legges til grunn at rikets sikkerhet er et dynamisk begrep, at det må tolkes ut fra den sammenhengen det står i, at det er beslektet med begrepet nasjonale sikkerhetsinteresser, som igjen vil ha likhetstrekk med begrepet nasjonale sikkerhetshensyn.

I NOU 1999:27[111] om forslag til ny Grunnlov[112] § 100 fremgår det at det må skilles mellom rikets sikkerhet og statens sikkerhet. Grl. § 100 og regulering av ytringsfrihet har lite til felles med Infoflytsystemet, men har det tilfelles at de begge dreier som om grunnleggende menneskerettigheter, jf. EMK art. 8 og 10, der «nasjonal sikkerhet» er et relevant formål for å gjøre inngrep i rettighetene. I NOU 1999:27 skilles det mellom «rikets sikkerhet» og «statens sikkerhet». Dette gjøres fordi det ikke vil være staten som utøvende organ eller internrettslig juridisk person som primært skal beskyttes, men selve nasjonen, eller riket, med dets territorium og forfatning.[113] Det fremgår at beskyttelsen også til en viss grad kan utvides til statsoverhode, regjering, samt forsvarsledelsen dersom det er krig. Trusselen kan komme både utenfra og innenfra, men målet må være å rokke nasjonens selvstendighet og forfatning.[114]

Etter dette tolkes nasjonale sikkerhetshensyn, sett i sammenheng med Infoflyt-systemet, å omfatte hensyn som ivaretar sikkerheten til statens grenser og forsvaret av landet, samt angrep som i hovedsak har til hensikt å rokke ved Norges selvstendighet og vår Grunnlov, herunder demokratiske verdier.

3.5.2.2 Redegjørelse for vilkåret «offentlig sikkerhet»

Vilkåret «offentlig sikkerhet» utgjør sammen med vilkåret «offentlig orden» en egen bestemmelse for utvisning etter utl. § 122. Begrepet er utdypet i rundskriv 2010-022 «Bortvisning og utvisning av EØS-borgere av hensyn til offentlig orden eller sikkerhet», i et eget pkt. 3.2.2.

[110] Jf. Ot.prp. nr. 75 (2006-2007) pkt. 18.1.1.
[111] NOU 1999:27 «Ytringsfrihet bør finde sted», forslag til ny Grl. § 100
[112] Jf. Kongeriket Norges Grunnlov (Grunnloven) av 17.5.1814
[113] Jf. NOU 1999:27 pkt. 6.3.2.1.
[114] ibid

Det fremkommer her at begrepene offentlig sikkerhet og offentlig orden er sammenfallende, og at begrepet offentlig sikkerhet angår statens ytre og indre sikkerhet, herunder bekjempelse av terrorisme, spionasje, revolusjonære opprør mv. Videre vil også bekjempelse av svært alvorlig kriminalitet som organisert kriminalitet eller alvorlig narkotikakriminalitet også kunne omfattes av begrepet. Terrorhandlinger etter strl. §§ 147a og 147 b, omfattes også av begrepet. I merknaden til bestemmelsen går det frem at offentlig sikkerhet langt på vei samsvarer med begrepet rikets sikkerhet, jf. Ot.prp. nr. 72 (2007-2008) pkt. 10.3. [115]

Ut fra det som ovenfor er nevnt kan det trekkes at offentlig sikkerhet angår forebygging og bekjempelse av svært alvorlig kriminalitet som har til hensyn å skade statens ytre og indre sikkerhet. Det kan også sluttes fra de ovennevnte forarbeidet at begrepet har likhetstrekk med begrepet «rikets sikkerhet». Disse kan altså gå noe over i hverandre.

3.5.2.3 Drøftelse av unntak for innsynsrett for å ivareta nasjonal og offentlig sikkerhet

I lovforslaget for regulering av Infoflyt-systemet er hensyn «til nasjonal- eller offentlig sikkerhet» alternative, men sidestilt i samme bokstav. Bestemmelsen dekker således både handlinger som rokker ved den norske selvstendighet og forfatning, og forebygging og bekjempelse av svært alvorlig kriminalitet. Videre angår vilkårene både indre og ytre sikkerhetstrusler, dvs. innenfor og utenfor de nasjonale grensene. Da annet ikke er nevnt, da lovens virkeområde er straffegjennomføring i Norge, og da det er andre lover som gjelder for eventuelt internasjonalt samarbeid, fremstår det som klart at det er tale om Norges sikkerhet i unntaket. Ettersom vilkårene er alternative vil det være tilstrekkelig for å benytte unntaket at det ene vilkåret er oppfylt. Ser man vilkåret offentlig sikkerhet isolert, dekker det flere av de samme av forbrytelsene som også dekkes av formålsbestemmelsen, og slik av unntaket i § 4h(2) bokstav a. Av dette er det nærliggende å tolke at bokstav b har en høyere terskel enn bokstav a, men dette er ikke klart.

For at unntaket fra innsynsrett skal kunne benyttes må det anses nødvendig. Det vises til redegjørelsen for nødvendighetsvurderingen i pkt. 3.5.1.2, der det fremgår at det skal foretas en

[115] Ot.prp. nr. 72 (2007-2008) Om lov om endringar i utlendingslovgivninga (reglar for EØS- og EFTA-borgarar o.a.)

konkret vurdering der det i denne sammenheng skal vurderes om innsynsnekt vil være egnet til å oppnå formålet nasjonal sikkerhet eller formålet offentlig sikkerhet, og om det vil være forholdsmessig å unnta innsynsrett satt opp mot det inngrepet dette vil utgjøre for den registrerte.

Det vil eksempelvis kunne anses som egnet til å oppnå formålet, dersom det vil kunne utgjøre en fare for nasjonal sikkerhet å gi den registrerte innsyn i opplysningene, da dette kan medføre at den registrerte varsler sine medsammensvorne, eller endrer planer og slik lykkes med disse. Derimot vil det ikke ansees som nødvendig dersom opplysningene allerede er gjort kjent gjennom media. Om det vil være forholdsmessig å vedta innsynsnekt vil avhenge av eksempelvis alvoret i situasjonen. Det skal uansett vurderes om det kan gis delvis innsyn.

Redegjørelsen av vilkårene nasjonal- og offentlig sikkerhet viser at det etter § 4h (2) bokstav b vil være tale om særlig alvorlig kriminalitet, og at dersom disse vilkårene først er oppfylt antakelig skal en del til for at det likevel gis innsyn. Loven stiller imidlertid krav om at dersom det kan gis delvis innsyn, eksempelvis i andre opplysninger som ikke har med de nevnte vilkårene å gjøre, så skal innsyn gis.

3.5.3 Unntak for innsynsnekt når opplysningene er utlevert fra PST

Etter strgjfl. § 4h (2) bokstav c kan innsyn nektes helt eller delvis dersom opplysningene er mottatt fra Politiets sikkerhetstjeneste (PST).[116] PST har som hovedformål å forebygge og motvirke trusler mot «rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser», jf. sikkerhetsloven § 1. Av merknadene til § 4h (2) bokstav c fremgår det at vitale nasjonale sikkerhetsinteresser er ment å dekke samtlige felter innenfor rikets totale sikkerhetsbehov.[117] Hvorfor disse opplysningene kan unntas og hvordan dette gir utslag, vil bli redegjort for i det følgende.

Hvorfor disse opplysningene skal unntas er knapt forklart i forslaget. Det går frem at opplysninger fra PST bør unntas av hensyn til sikkerhet, samt for å harmonisere reglene med politi-

[116] «Innsyn kan nektes helt eller delvis dersom opplysningene er mottatt fra politiets sikkerhetstjeneste.», jf. strgjfl. § 4h (2) bokstav c.

[117] Jf. Prop. 120 L (2013-2014) s. 32

registerloven § 66.[118] Etter polregl. § 66 er PST unntatt reglene om informasjonsplikt og innsyn etter polregl. §§ 48 og 49. Uttalelsene fra politiregisterloven er relevante for lovforslaget om Infoflyt fordi de nevnte bestemmelsene i polregl. og strgjfl. § 4h omhandler det samme, og fordi departementet har uttalt at dette bør føre til regellikhet mellom forslaget og politiregisterloven. Ettersom det er de samme hensynene som gjør seg gjeldende kan forarbeidene til politiregisterloven gi en forklaring på hvorfor opplysningene fra PST bør unntas også i Infoflyt-sammenheng.

I forarbeidene til politiregisterloven fremgår det at behovet for særregler for PST kommer av at deres samfunnsrolle er annerledes enn politiets.[119] Mens politiet tradisjonelt skal opprettholde ro og orden og utføre straffeforfølgning, arbeider PST i større grad enn politiet forebyggende, samt at de arbeider med saker som er særlig alvorlige og samfunnsskadelige, og som i ytterste konsekvens kan ramme landets sikkerhet og selvstendighet. Eksempler på slik kriminalitet er ulovlig etterretningsvirksomhet, spredning av masseødeleggingsvåpen, terrorisme og annen politisk motivert vold, som alle er svært alvorlige former for kriminalitet som kan utgjøre en fare for demokratiske verdier og strukturer. I tillegg nevnes organisert kriminalitet av langvarig karakter, der det kreves politiinnsats utover tradisjonell politietterforskning. Departementet uttaler i forarbeidene til politiregisterloven at PSTs opplysninger etter nærmere vurdering i de fleste tilfeller vil unntas innsynsrett, av hensyn til blant annet rikets sikkerhet, kildevern og metodebruk. Departementet uttaler videre til dette:

> «Hensett til at en eventuell innsynsrett på bakgrunn av det ovennevnte i realiteten ikke ville gi den registrerte muligheten til å føre kontroll med opplysninger om seg selv, kan departementet heller ikke se at lovforslaget til § 66 innebærer en svekkelse av personvernet.»[120]

Det legges altså opp til at de sakene som vil være relevante for PST å behandle, uansett vil være av en slik alvorlighetsgrad at de i de fleste tilfeller vil falle innunder et av de andre unntakene i innsynsbestemmelsen til Infoflyt-systemet, f.eks. § 4h (2) bokstav b og «nasjonal sikkerhet».

[118] Jf. Prop. 120 L (2013-2014) s. 32

[119] Jf. Ot.prp. nr. 108 (2008-2009) pkt. 17

[120] Jf. Ot.prp. nr. 108 (2008-2009) pkt. 17.4.3.

Til forskjell fra de andre unntakene i § 4h (2) legger ikke ordlyden opp til at det skal foretas noen nødvendighetsvurdering. Etter ordlyden i bokstav c skal det imidlertid vurderes om det kan gis delvis innsyn, og videre følger det av Norges folkerettslige forpliktelse at det skal foretas en nødvendighetsvurdering også her, jf. EMK art. 8 jf. mnskrl. §§ 2 og 3. Av merknad til § 4h (2) bokstav c kommer det frem at det ved vurdering av om det skal gis innsyn i disse opplysningene skal innhentes en vurdering fra PST.[121] Og det kan derfor tyde på at det skal foretas flere vurderinger før innsyn avslås etter denne bestemmelsen, enn det tilsynelatende ved første øyekast kan se ut til. Eksempelvis vil det kunne være anledning for å gi delvis innsyn der opplysningene er gamle og ikke lenger hemmeligholdte, eller der opplysningene ikke er av en slik karakter at det vil skade å gi innsyn. At nødvendighetsvurderingen ikke fremgår av ordlyden kan slik være uheldig rent lovteknisk, da det utfra sammenhengen kan se ut til at denne vurderingen ikke skal foretas, mens det etter en nærmere tolkning av bestemmelsen vil være krav om en slik vurdering likevel.

3.5.4 Svar på innsynsbegjæring

Den domfelte har krav på et svar på sin innsynsbegjæring. Ved innsynsnekt er det nærmere regulert hva dette svaret skal inneholde i strgjfl. § 4h (3) som lyder:

> «Dersom begjæringen om innsyn ikke tas til følge og det er grunnlag for kriminalomsorgen å unnlate å informere den registrere etter § 4g annet ledd, skal det gis et svar som ikke tilkjennegir at det foreligger en registrering i Infoflyt-systemet.»

Ordlyden i § 4h (3) tilsier at dersom det både er grunn til å unnta informasjonsplikt og innsyn, så skal det gis et svar som ikke tilkjennegir at vedkommende er registrert i Infoflyt-systemet. Ettersom vilkårene for unntak i bestemmelsene om informasjonsplikt og innsynsrett er like, vil det foreligge grunn til å unnta informasjonsplikt, dersom det er grunn til å unnta innsynsrett. Ved innsynsnekt skal det altså gis et svar som ikke tilkjennegir at det foreligger en registrering i Infoflyt-systemet, jf. § 4h (3).

[121] Jf. Prop. 120 L (2013-2014) s. 32

Årsaken til dette er antakelig at dersom det verken er vurdert sikkerhetsmessig forsvarlig å gi informasjon om registreringen eller innsyn i opplysningene, så kan et svar som bekrefter en registrering utgjøre en risiko i seg selv. Det er tenkelig at dersom den domfelte eksempelvis har planer om å gjennomføre en terroraksjon, men får vite at det lagres og systematiseres personopplysninger om han, kan endre sin adferd og eventuelt planer for gjennomføringen av aksjonen, og slik vanskeliggjøre sikkerhetstryggende arbeid i fengselet og i verste fall gjennomføre terroraksjonen.

For den registrerte er imidlertid dette problematisk, fordi han har en mistanke om at det kan forekomme registrering av personopplysninger. Å ikke få denne mistanken bekreftet eller avkreftet, kan i seg selv utgjøre en belastning. Hvor stor belastningen er, vil variere i størrelse med hvor mye den registrerte vet om Infoflyt-systemet og hvordan det fungerer, og om opplysningene har fått utslag for den enkelte i form av negative vedtak e.l. For den registrerte, som har fått et negativt vedtak med en begrenset begrunnelse, blir konsekvensen av dette at han fratas mulighet til å imøtegå de påstander som er rettet mot han, og til å korrigere eventuelle foreliggende feilregistreringer.

3.6 Innsynsregelen oppsummeres og settes opp mot gjeldende rett

Nedenfor følger en oppsummering av lovforslagets regel om innsynsrett, etterfulgt av en sammenligning med gjeldende rett.

Utgangspunktet er altså at den registrerte har krav på å få innsyn i opplysninger dersom han søker om det, men at det kan gjøres unntak fra dette utgangspunktet, helt eller delvis, dersom det etter en nødvendighetsvurdering ikke anses sikkerhetsmessig forsvarlig, eller dersom opplysningene er mottatt fra PST. Dersom det er fattet vedtak om innsynsnekt vil den registrerte få et svar som ikke tilkjennegir at han er registrert. Dermed får han ikke mulighet til å ivareta andre rettigheter som klage, retting og sletting.

Unntak fra innsynsretten kan være problematisk for den registrerte, fordi det medfører at han ikke har kontroll over egne personopplysninger, at han ikke får kontrollert opplysningskvaliteten, samt at det i et rettssikkerhetsperspektiv ikke anses som en god prosess at en ikke gis

anledning til å imøtegå de opplysningene som er registrert.[122] Mot dette står sikkerhetshensyn i vid betydning. I situasjoner der det står mellom å på den ene siden gi den domfelte et tilstrekkelig personvern og kontradiksjonsmulighet, og på den andre å hindre en større kriminell operasjon der mange menneskeliv kan gå tapt, vil hensynet til den domfeltes rettigheter måtte vike. Innsynsnekt imidlertid vurderes konkret, og det stilles krav om at innsyn vil stå i motstrid til å oppnå Infoflyt-systemets formål.

For de tilfellene der den registrerte får et svar som ikke tilkjennegir at han er registrert, er det viktig at det foreligger gode saksbehandlingsrutiner, som blant annet vil sikre at han tas ut av systemet når det ikke lenger er nødvendig at han er registrert, samt at det sikres at informasjonen som er registrert er korrekt og at eventuelle feil rettes. Dette er viktig for den registrerte fordi informasjonen kan utleveres til politiet, men også fordi informasjonen kan danne grunnlag for negative vedtak av stor betydning for soningsprogresjonen. Et svekket personvern og rettssikkerhet, må kompenseres med en styrket kontrolladgang.

Hvordan stiller så lovforslaget seg i forhold til gjeldende rett? Etter både gjeldende rett og etter lovforslaget er utgangspunktet at det etter begjæring til behandlingsansvarlig skal gis innsyn i opplysninger til den registrerte om ham selv. Unntakene er også langt på vei de samme i gjeldende rett og i lovforslaget. Det som hovedsakelig skiller reglene fra hverandre er at det etter popplyl. § 23 (3) stilles krav om at behandlingsansvarlig ved innsynsnekt må begrunne dette skriftlig med presis henvisning til hvilken unntakshjemmel som begrunner avslaget, mens det etter strgjfl. § 4h(3), ved unntak fra informasjonsplikten og innsynsretten, kun oppstilles et krav om at det skal gis et svar som ikke tilkjennegir at vedkommende er registrert i Infoflyt-systemet.

Etter personopplysningsloven vil den registrerte få innsyn i om han eksempelvis unntas innsyn av hensyn til «rikets sikkerhet, landets forsvar eller forholdet til fremmede makter eller internasjonale organisasjoner» jf. § 23 (1) bokstav a, eller om «det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare

[122] Ordet rettssikkerhet har mange sider, og benyttes på ulike måter, jf. Eckhoff og Smith, 2010 s. 58-59. Se også Stub, 2011 s. 30. I forvaltningssammenheng innebærer begrepet som regel beskyttelse mot overgrep og vilkårlighet fra myndighetenes side, forutberegnelighet, og mulighet til å ivareta sine rettslige interesser, jf. Bruce og Haugland, 2014 s. 26. Både legalitetsprinsippet, kontradiksjonsprinsippet og muligheter for kontroll ivaretar rettssikkerheten.

handlinger», jf. § 23 (1) bokstav b. Informasjonen om hvilken lovhjemmel som begrunner innsynsnekt vil ikke nødvendigvis røpe at vedkommende er registrert i Infoflyt-systemet, men opplysningen vil være egnet til å si noe om alvorlighetsgraden til de registrerte opplysningene. For den registrerte kan dette ha betydning f.eks. dersom han har mistanke om at det foreligger feil opplysninger, slik at han kan be om å få opplysningene kontrollert. På den andre siden kan det for kriminalomsorgen og politiet være kritisk at slik informasjon kommer ut, fordi det kan utgjøre en sikkerhetsrisiko dersom den Infoflyt-registrerte får kjennskap til denne informasjonen.

Ser man imidlertid hen til tidligere saksbehandlingspraksis etter strgjfl. § 7 (1) bokstav c og saksbehandlingsinstruks KSF 2/2005, der registrering i Infoflyt-systemet i seg selv kunne utgjøre begrunnelse for innsynsnekt, [123] utgjør lovforslaget ved strgjfl. § 4h en klar forbedring i den innsattes rettssikkerhet, med konkrete vilkår som må vurderes for innsynsnekt. Endringen sikrer at vilkårene blir vurdert, samt at det legger til rette for at det i ettertid kan føres kontroll med saksbehandlingen. Når det er sagt, er det likevel slik at selv om det stilles konkrete vilkår om hva som skal med i vurderingen, så åpnes det for stor grad av skjønn. Det er særlig tydelig i unntaksbestemmelsen § 4h (2) bokstav a, fordi oppfyllelse av vilkårene i formålsbestemmelsen kan danne grunnlag for unntak fra innsynsretten.

Formålsbestemmelsen i § 4f har i seg en rekke alternative vilkår som kan føre til registrering i Infoflyt-systemet. Vurderingen av om en person skal registreres i Infoflyt-systemet eller ikke er skjønnsmessige idet både beviskravet og vilkårene i formålsbestemmelsen må tolkes. Beviskravet er «grunn til å anta», jf. § 4f (1). Det foreligger verken veiledning i lov, forskrift, retningslinjer eller forarbeider hva gjelder sannsynlighetskravet «anta».[124] Storvik uttaler at begrepet omfatter de situasjoner der det foreligger konkrete og troverdige opplysninger som gir grunn til mistanke, og at det ikke er et krav at det foreligger sannsynlighetsovervekt.[125] Med andre ord stilles det ikke krav om at det må være mer sannsynlig at vedkommende vil begå eller medvirke til et av handlingsalternativene, enn at han ikke kommer til å gjøre det. Alvorlighetsgraden til de kriminelle handlingene som skal forebygges, forhindres og bekjempes blir således det avgjørende for om man kvalifiserer til å bli registrert.

[123] Se pkt. 2.2.

[124] Jf. Storvik, 2011, s. 102

[125] Jf. Storvik, 2011, s. 49

Som vist under pkt. 3.5.1 har § 4h (1) bokstav a i seg den realitet at dersom man først kvalifiserer til registrering i Infoflyt-systemet § 4f(1), kan dette i seg selv utgjøre begrunnelsen for innsynsnekt etter § 4h (1) bokstav a. Det som da skiller § 4h (1) bokstav a fra tidligere praksis etter KSF 2/2005 og strgjfl. § 7(1) bokstav c, er at det etter foreliggende lovforslag oppstilles objektive vilkår som må ligge til grunn i vurderingen om innsynsnekt. Denne endringen er positiv i den forstand at det stiller krav til hva som skal med i begrunnelsen, og slik gjør det enklere i ettertid å kontrollere at vilkårene har blitt vurdert.

Det kan tenkes at vid unntaksadgang og adgang til skjult registrering kan kompenseres ved gode kontrollmuligheter og klageadgang. Dette vil bli vurdert i det følgende.

4 Kontrollmuligheter og klageadgang

4.1 Innledning

Overfor er det redegjort for innsynsretten etter § 4h, og det fremkom av redegjørelse at lovforslaget åpner for en vid adgang til vedta innsynsnekt. Denne delen omhandler hvilke kontroll- og klagemuligheter den registrerte har i saker der det er vedtatt innsynsnekt. I pkt. 4.2 redegjøres det for Datatilsynets kontroll og virkemidler som er særskilt regulert i lovforslaget, før det i pkt. 4.3 redegjøres for hvilke andre muligheter for klage og kontroll som foreligger. I pkt. 4.4 følger en samlet vurdering av kontroll- og klagemuligheter, og en sammenligning mellom lovforslaget og gjeldende rett.

4.2 Datatilsynets kontroll og virkemidler jf. Prop. 120 L (2-13-2014)

Datatilsynet er et uavhengig forvaltningsorgan, jf. popplyl. § 42 (1). Dette innebærer at verken regjering eller departement kan gi Datatilsynet instruksjoner eller omgjøre avgjørelser fattet i enkeltsaker etter loven.[126] Det skilles mellom tilsynskompetanse og påleggskompetanse.[127] Med tilsynskompetanse menes at tilsynet har kompetanse til å føre tilsyn med behandlinger av

[126] Jf. Blixrud og Ottesen, 2010 s. 28

[127] Jf. Rapport 2012 s. 64

personopplysninger. Med påleggskompetanse menes Datatilsynets kompetanse til å gi pålegg om hvordan behandlingen skal gjøres etter personvernlovgivningen. Hvordan dette er regulert for Infoflyt redegjøres nedenfor. Vedtak fattet av Datatilsynet kan påklages til Personvernnemnda, jf. popplyl. §§ 42 (4) og 43 (1).

4.2.1 Rekkevidden av Datatilsynets kompetanse for tilsyn med Infoflyt-systemet

4.2.1.1 Datatilsynets tilsynskompetanse

Datatilsynets tilsynskompetanse reguleres i strgjfl. § 4j (1):

> «Datatilsynet skal etter begjæring fra den registrerte eller den som antar å være registrert, kontrollere at opplysningene om vedkommende er behandlet i samsvar med loven og at reglene om informasjonsplikt og innsyn er fulgt. Dette gjelder ikke opplysninger som kriminalomsorgen har mottatt fra Politiets sikkerhetstjeneste.»

Tilsynskompetansen innebærer at Datatilsynet kan kontrollere at behandlingen er i «samsvar med lov» og «at reglene om informasjonsplikt og innsyn er fulgt.» jf. strgjfl. § 4j (1)

Med «lov» menes straffegjennomføringslovens kapittel 1B og øvrige personvernregelverk, jf. strgjfl. § 4a. Datatilsynets kompetanseregler slik de er regulert i popplyl. kapittel 8 gjelder således også for kriminalomsorgen. Dette innebærer bl.a. at Datatilsynet har kompetanse til å kontrollere at vilkårene for registrering foreligger, samt at kriminalomsorgen overholder øvrige personvernregler som f.eks. kravene til informasjonssikkerhet. Datatilsynet har altså kompetanse til å kontrollere om kriminalomsorgen har overholdt regelverket, og vurdere konkret i den enkelte sak om det skulle ha vært gitt informasjon og/eller helt eller delvis innsyn.

Datatilsynet kan prøve lovanvendelsen, men ikke forvaltningens skjønn. Dette har sammenheng med at en jurist i Datatilsynet ikke vil ha et like godt grunnlag til å foreta sikkerhetsvurderinger som til enhver tid foretas i fengsel, sammenlignet med en jurist i kriminalomsorgen. At forvaltningens skjønn ikke kan overprøves gjør at behovet for klare og objektive kriterier for registrering og vurdering i Infoflyt blir desto viktigere, fordi slike krav gir anledning til å kontrollere at loven er fulgt. Nedenfor følger en gjennomgang av retten til å be Datatilsynet om kontroll.

Det følger av strgjfl. § 4j og merknad til bestemmelsen at en person, uavhengig av om han med sikkerhet vet at han er registrert i Infoflyt eller ikke, og uavhengig av om han tidligere har begjært innsyn, kan be Datatilsynet om å kontrollere behandling av personopplysninger i Infoflyt-systemet.[128] Retten er begrenset til bare å gjelde informasjon som eventuelt er registrert om vedkommende selv.

Retten til å be om kontroll, innebærer imidlertid ikke en rett til å få saken kontrollert. Datatilsynet er et tilsynsorgan og ikke et klageorgan, og kan etter henvendelse eller av eget tiltak uttale seg generelt eller konkret i spørsmål om behandling av personopplysninger, jf. popplyl. § 42 (3) nr. 7.[129] Det følger av forvaltningslovens veiledningsplikt i § 11 (1) at den registrerte som henvender seg til Datatilsynet uansett har krav på å få et svar på sin henvendelse, men at omfanget av veiledningen må tilpasses forvaltningsorganets situasjon og kapasitet. Samlet innebærer dette at selv om den registrerte har rett til å be om kontroll, så har ikke Datatilsynet plikt til å behandle saken, og det vil således være opp til tilsynets skjønn å vurdere om saken tas inn til behandling.

4.2.1.2 Unntak for opplysninger fra PST

Det er gjort unntak for Datatilsynets tilsynskompetanse for de tilfeller der kriminalomsorgen har mottatt opplysninger fra PST, jf. § 4j (1) siste punktum.

At det gjøres unntak fra Datatilsynets tilsynskompetanse for de tilfeller der opplysningene er utlevert fra PST har sammenheng med at det er Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjenesten (EOS-utvalget) som utøver tilsyn og kontroll med PST, jf. polregl. §§ 58 og 68, og sikkerhetsloven § 30. EOS-utvalget kan føre tilsyn av eget tiltak og ta klager til behandling, jf. EOS-loven § 3.[130] I forarbeidene til politiregisterloven vurderer departementet det dithen at den registrertes personvern er tilstrekkelig ivaretatt gjennom adgangen til å be EOS-utvalget om kontroll av behandling av personopplysninger i PST.[131]

[128] Jf. Prop. 120 L (2013-2014) s. 32
[129] Jf. Rapport 2012 s. 63 og Prop. 120L (2013-2014) s. 28
[130] EOS-loven, lov av 2.3.1995 nr. 7
[131] Jf. Ot.prp. 108 (2008-2009) pkt. 17.4.3.

For at den registrerte skal kunne be EOS-utvalget om kontroll, må han imidlertid forutsetningsvis kjenne til Infoflyt-systemet, vite at det er mulig at han er registrert der, og til slutt ha kunnskap om at han kan kontakte EOS-utvalget for kontroll. Da utlevering av opplysninger fra PST til kriminalomsorgen kan begrunne unntak fra både informasjonsplikt og innsynsrett, vil de ovennevnte forutsetningene i mange tilfeller ikke foreligge.

4.2.1.3 Svar på Datatilsynets kontroll

Den domfelte har krav på et svar fra Datatilsynet ved kontroll. Svaret er imidlertid underlagt begrensninger i enkelte tilfeller. Begrensningen er regulert i strgjfl. § 4j (2) som lyder:

> «Har kriminalomsorgen eller politiet besluttet unntak fra informasjonsplikten etter § 4g annet ledd eller politiregisterloven § 48, skal ikke svaret tilkjennegi at det foreligger en registering i Infoflyt-systemet.»

Etter denne bestemmelsen er Datatilsynet forpliktet til å gi et nøytralt svar for de tilfellene der kriminalomsorgen eller politiet har besluttet å ikke følge informasjonsplikten, jf. §§ 4g(2) eller polreg. § 48. Dette innebærer at dersom en innsatt har fått innsynsnekt i tråd med § 4h (2), og har fått et svar som ikke tilkjennegir at han er registrert jf. § 4h (3), etter begjæring hos Datatilsynet må få et svar som ikke viser at han er registrert. Den registrerte vil således få vedtaket kontrollert av Datatilsynet, men ikke få bekreftet eller avkreftet at han er registrert.

Som tidligere vist kan det være gode grunner som taler for at den innsatte ikke får kunnskap om registreringen. For den registrerte kan imidlertid et slikt svar oppleves belastende i seg selv, fordi man verken vet omfanget av registreringen eller utfall av behandlingen, eksempelvis om opplysningene blir utlevert. Det kan også tenkes at den innsattes tillitt til forvaltningen svekkes av at han verken får bekreftet eller avkreftet registrering i Infoflyt-systemet. Svekket tillitt til forvaltningen kan eksempelvis gå utover kriminalomsorgens rehabiliteringsarbeid i fengselet, fordi det i stor grad er avhengig av medvirkning fra den innsatte og hans tillitt til de ansatte. [132]

[132] Jf. strgjfl. § 3 (1) 2 og 3.pkt. Se også Storvik, 2011 s. 37

4.2.1.4 Oppsummert om Datatilsynets tilsynskompetanse

Oppsummert kan en si om rekkevidden av Datatilsynets tilsynskompetanse at den registrerte har rett til å be om å få sin sak kontrollert, men at utfallet av begjæringen vil avhenge av om Datatilsynet har kompetanse til å behandle saken, samt at Datatilsynet prioriterer behandling av den. For de tilfellene som ikke blir tatt til behandling, vil den registrerte være avhengig av andre tilsyn som kan utføre kontroll, eksempelvis Sivilombudsmannen eller EOS-utvalget. Dette forutsetter at den registrerte kjenner til ombudsmannen og utvalgets funksjon, samt at han har ressurser til å ta kontakt med dem.

For de tilfellene der Datatilsynet tar saken til behandling, vil kriminalomsorgens saksbehandling bli kontrollert. I saker der kriminalomsorgen har fulgt informasjonsplikten i strgjfl. § 4g (1), men har unntatt innsynsretten jf. § 4h (2), vil den registrerte ved klage til Datatilsynet få et svar som tilkjennegir at han er registrert. I disse tilfellene vet den registrerte at han er registrert, og Datatilsynets svar vil således ikke avsløre informasjon som den registrerte ikke allerede kjenner til. For de tilfellene kriminalomsorgen eller politiet har unntatt informasjonsplikten, jf. strgjfl. § 4g (2) eller polregl. § 48, skal datatilsynet gi et nøytralt svar. Hva Datatilsynet så kan gjøre, dersom de finner at loven ikke er fulgt, redegjøres for i neste punkt om tilsynets påleggskompetanse.

4.2.2 Har Datatilsynet påleggskompetanse?

Utgangspunktet er at Datatilsynet har full påleggskompetanse, jf. popplyl. § 46. Dette innebærer at tilsynet kan gi pålegg om endring eller opphør av ulovlig behandling.[133] Eksempler på slik dette kan være feil ved informasjonssikkerheten.[134] I lovforslaget er det imidlertid gjort unntak fra Datatilsynets påleggskompetanse etter strgjfl. § 4j (3) og lyder som følger:

[133] Da oppgavens problemstilling angår innsynsrett, og kontroll av den, vil Datatilsynets generelle påtalekompetanse ikke bli problematisert ytterligere.

[134] Jf. Prop. 120 L (2013-2014) s. 28

> «Datatilsynet kan ikke gi pålegg om innsyn i opplysninger som kriminalomsorgen eller politiet har unntatt fra innsynsretten etter § 4h annet ledd eller politiregisterloven § 49 fjerde ledd.»

For de tilfeller der kriminalomsorgen eller politiet har unntatt den registrerte fra innsynsrett, er Datatilsynet unntatt påleggskompetanse. Datatilsynets kontroll av kriminalomsorgens vedtak om innsynsnekt medfører således ikke annet enn at saksbehandlingen blir kontrollert. Det fremkommer av merknad til bestemmelsen at for de tilfeller der Datatilsynet finner at kriminalomsorgens lovanvendelse er feil, skal tilsynet gi skriftlig melding til behandlingsansvarlig.[135] Meldingen skal være begrunnet og skal følges opp av behandlingsansvarlig med en fornyet vurdering av innsynsspørsmålet.[136] Dermed sikres den registrerte en fornyet vurdering og eventuelt en omgjøring av vedtaket, jf. fvl. § 35. Rent lovteknisk vil det være positivt om innholdet i ovennevnte merknad til bestemmelsen tas inn i forskriftsform, jf. strgjfl. § 4k bokstav o),[137] da det vil medføre oversiktlighet for saksbehandler, og forutberegnelighet og klarere rettigheter for den registrerte.

Det er altså gjort unntak fra Datatilsynets påleggskompetanse ved innsynsnekt. Begrensningen som følger av § 4j (3) er lik begrensningen for Datatilsynets kompetanse til å gi pålegg etter polregl. § 60 (1) 3 pkt., se også forskrift § 42-3. Selv om ikke forarbeidene til politiregisterloven er gjeldende for Datatilsynets påleggskompetanse i Infoflyt-saker, kan det trekkes paralleller til argumentasjonen i politiregisterlovens forarbeider, fordi de samme hensyn om spesialkunnskap gjør seg gjeldende.

I politiregisterloven med forskrift skilles det mellom politiets påleggs- og anmerkningskompetanse, der det kun er påleggskompetansen som er bindende for den behandlingsansvarlige.[138] Av forskrift til politiregisterloven fremgår det at det ved anmerkning fra Datatilsynet forutsettes at den behandlingsansvarlige vurderer tilsynets anmerkning og kontrollerer om det

---

[135] Jf. Prop. 120 L (2013-2014) s. 32

[136] Jf. Prop. 120 L (2013-2014) s. 32

[137] Strgjfl. § 4k: «Kongen kan gi forskrift om a) behandlingsansvar, b) type opplysninger som kan behandles, c) opplysningskvalitet, d) tilgang, e) samarbeid med politiet, f) fremgangsmåte ved opprettelse og avslutning av sak, g) informasjonsplikt, h) innsyn, i) retting, sperring og sletting, j) handleplikt ved feil eller mangler, k) oppbevaring og bruk av sperret informasjon, l) utlevering av informasjon til politiet, m) saksbehandlingsregler, n) klage og klagefrist, o) tilsyn, p) informasjonssikkerhet og internkontroll.»

[138] Jf. Ot.prp. nr. 108 (2008-2009) kap. 21 merknad til § 60

har forekommet uregelmessigheter i forbindelse med behandling av opplysninger, og videre at den behandlingsansvarlige gir tilbakemelding til tilsynet om hva som ble utfallet av kontrollen.[139] Begrunnelsen for at Datatilsynet ikke er gitt påleggskompetanse i disse innsynssakene er ifølge forarbeidene at unntak fra innsynsrett baseres på en politifaglig vurdering, og at tilsynet derfor ikke burde kunne binde politiet i slike avgjørelser.[140] Det pekes også på at eventuelle uriktige avgjørelser fra Datatilsynet vil kunne få skadevirkninger, ved at for eksempel personers sikkerhet settes i fare.[141] Det kan trekkes paralleller fra denne begrunnelsen til saker om innsynsnekt i Infoflyt-systemet, da Datatilsynet ikke vil ha et like godt grunnlag for å foreta sikkerhetsvurderinger for fengselet sammenlignet med en jurist i kriminalomsorgen.

Det konkluderes i forarbeidene til politiloven med at politiet i praksis har kontroll med seg selv i innsynssaker.[142] Dette vil således også gjelde for kriminalomsorgen. Helt overlatt til seg selv er den imidlertid ikke dersom løsningen blir slik det antydes i merknaden til bestemmelsen, at Datatilsynet gis anmerkningskompetanse. Slik anmerkningskompetanse vil imidlertid ha mindre gjennomslagskraft enn påleggskompetanse ettersom den ikke er bindende.

Oppsummert innebærer strgjfl. § 4j at Datatilsynet som utgangspunkt har full påleggskompetanse. Kompetansen er imidlertid innskrenket for de tilfeller der politiet eller kriminalomsorgen har avslått krav om innsyn etter strgjfl. § 4h(2) eller polregl. § 48. I slike tilfeller kan Datatilsynet gis anmerkningskompetanse, men slik kompetanse vil ikke være bindende for kriminalomsorgen. Spørsmålet er så om Datatilsynets manglende påleggskompetanse kan kompenseres med andre kontrollmuligheter. Dette vil bli behandlet i det videre.

[139] Jf. Ot.prp. nr. 108 (2008-2009) kap. 21 merknad til § 60
[140] Jf. Ot.prp. nr. 108 (2008-2009) kap. 21 merknad til § 60
[141] Jf. Ot.prp. nr. 108 (2008-2009) kap. 21 merknad til § 60
[142] Jf. Ot.prp. nr. 108 (2008-2009) kap. 21 merknad til § 60

4.3 Andre kontroll- og klagemuligheter

4.3.1 Innledning

Nedenfor redegjøres det kort for andre klage og kontrollmuligheter som er relevante ved kontroll av enkeltsaker, jf. strgjfl. § 4h (2). Dette er henholdsvis Sivilombudsmannen, overordnet forvaltningsorgan, domstolen og Den Europeiske menneskerettighetsdomstol.

4.3.2 Sivilombudsmannens kontroll

Kontroll fra Sivilombudsmannen kan initieres ved at den registrerte selv klager til Sivilombudsmannen,[143] eller ved at ombudsmannen fører kontroll av eget tiltak.[144] Ombudsmannens uttalelser er i utgangspunktet ikke bindende,[145] men blir tradisjonelt vist stor respekt i forvaltningen, og hans uttalelser blir som regel tillagt stor vekt som rettskilde i kriminalomsorgen.[146] Ombudsmannssak 2007/264 er et eksempel på at kriminalomsorgen endret sin Infoflyt-praksis på bakgrunn av en Sivilombudsmannssak. Ombudsmannen avgjør om en sak tas inn til behandling, og den registrerte har således ikke rett til å få sin sak behandlet.[147]

For å ha adgang til å klage til Sivilombudsmannen må man i utgangspunktet ha uttømt alle andre klagemuligheter, jf. § 6 jf. fvl. § 1.[148] Dette innebærer at den registrerte ikke kan klage til Sivilombudsmannen før han har fått svar fra KDI. Er eksempelvis vedtak fattet på lokalt nivå i fengselet jf. strgjfl. § 6 (1), kan det ta lang tid fra behovet om innsyn oppstår til man eventuelt får et svar på en klage hos Sivilombudsmannen. Det tilføyes at Sivilombudsmannen ikke har myndighet til å omgjøre forvaltningens vedtak, og at han har taushetsplikt om de opplysningene han får tilgang til i sin tjeneste.[149] Det vil imidlertid innebære en trygghet for

[143] Jf. sivilombudsmannsloven § 4, lov av 22.6.1962 nr. 8

[144] Jf. sivilombudsmannsloven § 5

[145] Jf. sivilombudsmannsloven § 10

[146] Jf. Storvik, 2011 s. 30

[147] Jf. sivilombudsmannsloven § 6 (4)

[148] Unntaksvis kan man klage til Sivilombudsmannen ved brudd på forvaltningslovens regler om alminnelig saksbehandling, jf. fvl. kap. III. Se f.eks. ombudsmannssak 2007/497 der en innsatt som var registrert i Infoflyt klagde til Sivilombudsmannen over kriminalomsorgens saksbehandlingstid og manglende skriftlige tilbakemeldinger i forbindelse med søknad om permisjon.

[149] Jf. sivilombudsmannsloven § 9

den registrerte å få sin sak kontrollert, uavhengig av om han får sin mistanke om registrering bekreftet eller ikke, da han vet at saken blir uavhengig kontrollert.

Kort oppsummert har altså Sivilombudsmannen innsyn i opplysningene, men taushetsplikt overfor bl.a. den registrerte. Hans anbefalinger er ikke bindende, men blir stort sett fulgt. Sivilombudsmannen er uavhengig og er således et utenforliggende kontrollorgan, men han har ikke kompetanse til å pålegge kriminalomsorgen å omgjøre et vedtak om innsynsnekt, og vil således ikke ha effektiv kontroll ved prøvingen av et vedtak.

4.3.3 Klageadgang til overordnet forvaltningsorgan

Klageadgang er kun omtalt i lovforslaget ved en henvisning til den generelle klageadgangen til overordnet organ i medhold av fvl. 28 jf. strgjfl. § 7.[150] Dette innebærer at vedtak fattet på regionalt nivå etter strgjfl. § 6 (2), har KDI som klageorgan, mens det er Justis- og beredskapsdepartementet som eventuelt behandler klager over vedtak fattet av KDI.[151]

Klageorganet har kompetanse til å prøve alle sidene av saken og kan også ta hensyn til nye omstendigheter, jf. fvl. § 34. En slik realitetsavgjørelse innebærer at det overordnede organ kan overprøve det underordnede forvaltningsorganets skjønn.[152] Det overordnede organ foretar altså en ny vurdering basert på den situasjonen som foreligger på tidspunktet for klagen. Klageorganet kan velge mellom å fatte nytt vedtak, eller å oppheve foreliggende vedtak for så å sende saken tilbake for ny behandling, jf. 34 (4). Det kan imidlertid spørres om en slik overprøving likevel vil være helt uavhengig av tidligere prøving, da overprøvingen enten skjer innad i kriminalomsorgen eller av Justis- og beredskapsdepartementet. Det kan synes som oppfatningen til FNs arbeidsgruppe mot vilkårlig fengsling i sin rapport mente at slik overprøving ikke er uavhengig av underinstansens vurdering, da de etter sitt besøk i Norge våren 2007 kritiserte at ingen utenforliggende kontrollorgan, med unntak av Sivilombudsmannen, fikk innsyn i opplysningene ved innsynsnekt.[153]

[150] Jf. Prop. 120 L (2013-2014) s. 28
[151] Jf. Prop. 120 L (2013-2014) s. 28
[152] Jf. Eckhoff og Smith, 2010 s. 322
[153] Jf. Rapport A/HRC/7/4/Add.2

4.3.4 Domstolsprøving

Det er et ulovfestet prinsipp at domstolen skal kunne prøve forvaltningsavgjørelser. Domstolen er et uavhengig statlig organ som i forvaltningssaker spiller en viktig rolle for å sikre at den enkelte borger får sine rettigheter oppfylt og for å forhindre at det skjer feil. Domstolen kan etter dette prinsippet føre legalitetskontroll, om det er begått feil ved saksbehandlingen og om avgjørelsen bygger på riktig faktisk grunnlag. [154] Domstolen kan i utgangspunktet ikke prøve forvaltningens frie skjønn, med mindre det foreligger såkalt myndighetsmisbruk ved usaklig forskjellsbehandling, ved at det er tatt utenforliggende hensyn, eller om det foreligger vilkårlige eller sterk urimelige avgjørelser.[155]

I det følgende vil to forutsetninger for domstolskontroll trekkes frem, henholdsvis klare regler og domstolens innsynsrett. Ettersom domstolen i hovedsak ikke kan prøve forvaltningsskjønnet, er det en forutsetning at lovteksten stiller klare krav til hvilke vilkår som skal behandles. Som vist i pkt. 3.5 stiller innsynsbestemmelsen i strgjfl. § 4h (2) krav om at det skal foretas en nødvendighetsvurdering. Det er positivt for både praktiseringen av regelen og for kontrollen av forvaltningens etterlevelse av den, at nødvendighetsvurderingen tas inn i lovteksten.[156] Domstolen kan prøve om forvaltningen har foretatt en riktig nødvendighetsvurdering, men kan i utgangspunktet ikke prøve forholdsmessigheten. Videre oppstiller også formålsbestemmelsen en rekke objektive vilkår som domstolen også kan prøve, jf. strgjfl. § 4f (1) bokstavene a til e. For at domstolen skal kunne utelukke at det foreligger myndighetsmisbruk, er det imidlertid en forutsetning at domstolen har adgang til de opplysningene som forvaltningen har fattet sin beslutning på.

Som vist i forrige punkt kritiserte FNs arbeidsgruppe mot vilkårlig fengsling det norske prøvingssystemet idet Sivilombudsmannen var det eneste utenforliggende organ som fikk adgang til opplysningene i saker der kriminalomsorgen hadde ilagt innsynsnekt av sikkerhetsmessige årsaker. Arbeidsgruppen presiserte at Høyesterett hadde akseptert at domstolene ikke skulle ha adgang, og at den registrerte dermed ikke fikk en reell mulighet til å imøtegå de påstander som var reist mot han.

---

[154] Jf. Innjord, 2004 s. 728

[155] Jf. Kjønstad og Syse, 2010 s. 247

[156] Jf. Norges folkerettslige forpliktelse f.eks. EMK art. 8 (2) og 95/46/EF art. 6 (1) bokstav c

Hvilken høyesterettssak arbeidsgruppen sikter til kommer ikke frem av rapporten, men det er trolig at det siktes til Rt. 2006 s. 1300.[157] Rt. 2006 s.1300 gjaldt domstolens prøvingsrett av forvaltningsvedtak om isolasjon[158] i fengsel ved avdeling med særlig høyt sikkerhetsnivå. Vesentlige deler av grunnlaget for vedtaket var unntatt innsynsrett for den innsatte, jf. strgjfl. § 7 bokstav c og d, og videre for domstolene i sak om prøving av vedtakets lovlighet, jf. tvistemålsloven § 204 nr. 2.[159] Høyesterett pekte på at den innsatte hadde klage og overprøvingsadgang og at rettssikkerheten derfor var ivaretatt. Retten uttalte videre at systemet med høyrisikoavdelinger ville bryte sammen dersom kriminalomsorgen ved et saksanlegg skulle tvinges til å legge frem taushetsbelagte opplysninger. Høyesterett kom til at det i saken ikke forelå en rett til innsyn eller plikt til å begrunne vedtaket, og vedtaket ble ikke kjent ugyldig.

Disse argumentene ble også trukket frem av Infoflyt-utvalget i deres uttalelse om domstolsprøving, da politiarbeidet kan bli skadelidende ved at sensitive opplysninger tilkommer partene i sivile saker.[160] Av Infoflyt-utvalgets rapport fremkommer det at frykt for at den registrerte skal få kunnskap om at det registreres opplysninger om han i Infoflyt-systemet, har medført at politiet har vært tilbakeholdne med å gi informasjon til kriminalomsorgen.[161] Også etter den nye tvisteloven (heretter tvl.) § 22-3 er utgangspunktet at det ikke kan føres bevis som krenker lovbestemt taushetsplikt. I tråd med sitt mandat vurderte Infoflyt-utvalget om det er behov for endringer av innsynsreglene i tvl. § 23.[162]

På bakgrunn av utvalgets funn ble det fremmet forslag om utredning av om tvisteloven burde endres til å få en lignende ordning som i strprl. § 242a (jf. tidligere tvistemålsloven § 204[163]) om vitneforklaring.[164] En slik ordning vil medføre at domstolen får innsyn i opplysningene, men at den registrerte og hans advokat kan nektes innsyn. Dommeren vil da få innsyn i vurderingene, og settes i stand til å prøve forvaltningens lovanvendelse. Sammenlignet med dagens

[157] Se også Løvdal 2010 s. 73

[158] Isolasjon reguleres i strgjfl. § 37. Loven benytter begrepet «utelukkelse fra fellesskapet», og oppstiller alternativene «helt eller delvis».

[159] Tvistemålsloven er opphevet, men § 204 nr. 2 er i hovedsak videreført i lov av 17.6.2005 nr. 90 § 22-3.

[160] Jf. Rapport 2012 s. 76

[161] Jf. Rapport 2012 s. 70 og 76

[162] Jf. Rapport 2012 s. 76

[163] Tvistemålsloven, lov av 13.8.1915 nr. 6. Opphevet.

[164] Jf. Rapport 2012 s. 76-77

ordning der dommeren kun får en vag og intetsigende redegjørelse av hensyn til sikkerhet, [165] vil en slik ordning kunne gi den registrerte rettssikkerhet i form av utenforliggende kontroll. Da en slik lovendring også kan være relevant i andre saker, som for eksempel for utlendingsmyndighetens mulighet til å motta informasjon fra politiet, anbefalte Infoflyt-utvalget at dette utredes nærmere på et bredere grunnlag enn utvalgets mandat.[166] Utvalgets anbefaling er nevnt, men ikke ytterligere kommentert i lovforslaget fra departementet.

Infoflyt-utvalget vurderte også om ordning med skjult advokat etter mønster fra strprl. § 100a kunne være et alternativ i Infoflyt-saker.[167] I saker der retten har besluttet innsynsnekt for partene, kan det etter strprl. § 100a oppnevnes en advokat som under taushetsplikt blir gjort kjent med opplysningene. I straffesaken kan advokaten da angripe et vedtak der de skjulte opplysningene kunne vært brukt som grunnlag for en mildere eller frifinnende dom. Infoflyt-utvalget foreslo imidlertid ikke en slik ordning, fordi skjult advokat ikke er et alternativ i sivile saker fra før, og fordi det mente at Infoflyt-saker ikke var av en slik art eller omfang at det tilsa at det skulle innføres en slik ordning i bare slike saker.[168] Departementet har ikke kommentert utvalgets konklusjon, utover å vise til den i lovforslaget.[169] Da det ser ut til å mangle andre løsninger der sakens opplysninger kan kontrolleres, kan det spørres om dette burde utredes nærmere. Det avgrenses mot å gå inn på en nærmere drøftelse av spørsmålet, men bemerkes at det for en advokat som ikke kan samtale med sin klient for å verifisere opplysningene, vil få en vanskelig oppgave med å kontrollere om opplysningene stemmer. På den annen side vil en slik advokat kunne kontrollere kildene og opplysningenes kvalitet. I mangel av annen utenforliggende kontroll, vil skjult advokat kunne være bedre enn ingen kontroll.

Det nevnes kort at den registrerte også kan klage sin sak inn for Den Europeiske menneskerettighetsdomstol, jf. EMK art. 8 og 34. Prosessen med å klage til EMD krever imidlertid at man har uttømt de nasjonale rettsmidler før saken kan tas til behandling, jf. EMK art. 35 nr. 1. Det vil derfor ta lang tid fra behovet melder seg om innsynsrett for den innsatte, og til han eventu-

[165] Jf. Rapport 2012 s. 77, jf. sitat «I dag er det fare for at et begrunnet avslag vil være intetsigende eller vagt (…)»

[166] Jf. Rapport 2012 s. 76-77

[167] Jf. Rapport 2012 s. 78

[168] Jf. Rapport 2012 s. 78

[169] Jf. Prop. 120 (2013-2014) s. 28

elt kan ta saken til EMD. På veien dit vil de ovennevnte kontrollmuligheter således være viktigere for den enkelte innsatt, og av plasshensyn vil dette derfor ikke bli drøftet nærmere.

Infoflyt-utvalgets funn viser at det er behov for å kunne unnta innsynsrett i særlig alvorlige saker av hensyn til sikkerhet i vid forstand. Lovforslagets objektive vilkår og krav om nødvendighetsvurdering, gjør etterprøvbarhet mulig på et forvaltningsområder som er preget av skjønnsmessige vurderinger. Etterkontroll forutsetter imidlertid at kontrolløren får innsyn i de opplysninger som danner grunnlag for resultatet. Foreliggende lovforslag åpner verken for at domstolen skal gis innsyn i disse opplysningene eller at den registrerte gis en skjult advokat som kan sikre at loven er fulgt. For den registrerte kan manglende kontroll med forvaltningen svekke tillitten til at det er foretatt en fullgod vurdering, samt at det kan føre til at vedtak som fattes med grunnlag i opplysningene blir feil. Videre kan manglende kontroll føre til at det forplanter seg en praksis som ikke er i overenstemmelse med loven. En ordning lik strprl. § 242 a der domstolen får innsyn i opplysningene vil kunne bøte på denne svakheten ved lovforslagets ordning. Etter dette er det usikkert om det foreligger uavhengig utenforliggende kontroll som tilstrekkelig ivaretar den registrertes rettssikkerhet.

4.4 Kontrollmuligheter og klageadgang i lovforslaget oppsummeres og settes opp mot gjeldende rett

Oppsummert kan en si at Datatilsynet og Sivilombudsmannen kan føre uavhengig kontroll med Infoflyt-systemet, men at kontrollen ikke er fullgod når føringene ikke er bindende for kriminalomsorgen. Domstolen kan foreta utenforliggende kontroll, og den kan kjenne et vedtak ugyldig, men kontrollen blir ikke reell når domstolen ikke gis innsyn i opplysningene som har ført til innsynsnekt.

Mulighetene for kontroll og klageadgang etter gjeldende rett skiller seg fra lovforslaget ved at Datatilsynets har full påleggskompetanse også i saker om innsynsnekt, jf. §§ 46 flg. Datatilsynet har således lik tilsynskompetanse i lovforslaget og etter gjeldende rett, men tilsynets gjennomslagskraft overfor forvaltningen er dårligere i lovforslaget fordi det etter disse reglene er unntatt påleggskompetanse.

Hva gjelder domstolens prøvelsesrett er denne lik i lovforslaget og etter gjeldende rett. Da lovforslaget imidlertid fremstår som mer oversiktlig og enhetlig enn gjeldende rett, samt stil-

ler objektive vilkår og krav til nødvendighetsvurdering, kan lovforslaget medføre at det blir enklere å føre etterfølgende kontroll. Som overfor vist er imidlertid prøvingen begrenset av at domstolen ikke gis innsyn i opplysningene som ligger til grunn for vedtak om innsynsnekt.

Selv om utgangspunktet er at det foreligger en rekke utenforliggende organer som kan føre kontroll med Infoflyt-systemet, medfører unntakene fra kontrolladgang i innsynssaker usikkerhet om kontrollen blir reell.

5 Avsluttende bemerkninger

I saker om særlige alvorlige kriminalitet kan det være en forutsetning for at kriminalomsorg og politi skal kunne utføre sine oppgaver at den domfelte ikke kjenner til at han er registrert, hvilke opplysninger som er registrert, hvordan de er behandlet mv. I avveiningen mellom den enkelte domfeltes kontroll over egne opplysninger og samfunnets sikkerhet i vid forstand, må kanskje egenkontrollen vike. Tidligere kritikk av Infoflyt-systemet og Infoflyt-utvalgets rapport viser imidlertid at det er et behov for utenforliggende kontroll med systemet, både av hensyn til informasjonssikkerhet og av hensyn til saksbehandlingsrutiner.

Det er overfor vist at den registrerte i utgangspunktet har innsynrett, men at kriminalomsorgen gis vid adgang til å unnta retten. Når vilkårene for å unnta innsyn samsvarer med vilkårene for å registreres i Infoflyt-systemet, kan resultatet bli at ingen av de registrerte i Infoflyt-systemet gis innsyn. Lovforslagets krav om nødvendighetsvurdering og objektive vilkår er imidlertid positivt både for den innsatte og for saksbehandler, da dette stiller tydeligere krav til innholdet i vurderingen sammenlignet med gjeldende rett. Et klarere rettsgrunnlag er også enklere å kontrollere.

Det er en rekke utenforliggende organer som kan kontrollere Infoflyt-systemet, men ingen av dem er gitt forutsetninger som setter dem i stand til å foreta kontrollen fullt ut. Sivilombudsmannen er gitt innsyn, men kan ikke fatte bindende avgjørelser. Datatilsynet er også gitt innsyn, men er unntatt påleggskompetanse. Overordnet forvaltningsorgan er både gitt innsyn og kan fatte bindende avgjørelser, men det kan stilles spørsmål ved deres uavhengighet. Og domstolen kan fatte bindende avgjørelse, men gis ikke innsyn. Da Infoflyt-systemet benyttes som

opplysningsgrunnlag for risikovurderinger ved beslutningstaking i kriminalomsorgen, kan fraværet av kontroll være problematisk i et rettssikkerhetsperspektiv. Slik reglene om innsynsrett og kontroll er utformet i lovforslaget vil den enkeltes mulighet for kontradiksjon være avskåret. En utredning om endring av tvisteloven som overfor vist, bør etter dette snarlig gjennomføres. I tillegg til en slik utredning støttes herved Infoflyt-utvalget anbefaling om en grundig evaluering av Infoflyt-systemet etter at det har vært i drift i 2-4 år.[170]

[170] Jf. Rapport 2012 s. 87

6 Litteraturliste

6.1 Lov

1814 Kongeriket Norges Grunnlov (Grunnloven), 17.5.1814

1905 Alminnelig borgerlig straffelov (straffeloven) av 22.5.1905 nr. 10

1962 Lov om Stortingets ombudsmann for forvaltningen (Sivilombudsmannsloven) av 22.6.1962 nr. 8

1967 Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) av 10.2.1967 nr. 2

1995 Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-loven) av 2.3.1995 nr. 7.

1998 Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) av 20.3.1998 nr. 10

1999 Lov om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven) av 21.5.1999

2000 Lov om behandling av personopplysninger (personopplysningsloven) av 14.4.2000 nr. 31

2001 Lov om gjennomføring av straff mv. (straffegjennomføringsloven) av 18.5.2001 nr. 21

2005 Lov om meling og rettergang i sivile tvister (tvisteloven) av 17.6.2005 nr. 90

2006 Lov om rett til innsyn i dokument i offentleg verkstemd (offentleglova) av 19.05.2006 nr. 16

2010 Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) av 28.5.2010 nr. 16

6.1.1 Opphevet lov

1915 Lov om rettergangsmåten for tvistemål (tvistemålsloven) av 13.8.1915 nr.6 § 204 nr. 2

6.2 Forskrift, retningslinjer og rundskriv

2013 Forskrift om behandling av personopplysninger i kriminalomsorgen (forskrift om behandling av personopplysninger i kriminalomsorgen) av 20.9.13 nr. 1099

2002 Forskrift til lov om straffegjennomføringsloven (straffegjennomføringsforskriften) av 22.2.2002 nr. 183

2000 Forskrift om behandling av personopplysninger (personopplysningsforskriften) av15.12.2000 nr. 1265

2002 Retningslinjer til lov om gjennomføring av straff mv. (straffegjennomføringsloven)og til forskrift til loven. Fastsatt av Kriminalomsorgens sentrale forvaltning 16.5.2002 med hjemmel i forskrift til lov om straffegjennomføring av 22.2.2002 § 7-1. Revidert 27.10.2008.

2011 Rundskriv fra Utenriksdirektoratet, RS 2010-022, om bortvisning og utvisning av EØS-borgere av hensyn til offentlig orden eller sikkerhet av 20.07.2011.

2005 Rundskriv fra Justis- og politidepartementet, G-3/2005, om Informasjonsutveksling mellom kriminalomsorgen og politiet/påtalemyndigheten av 18.03.2005.

2005 Rundskriv fra Kriminalomsorgens sentrale forvaltning, KSF 2/2005, om INFOFLYT – særskilt saksbehandlingsinstruks.

6.3 Traktater og direktiver

1950 Den Europeiske menneskerettighetskonvensjonen (EMK), 4.11.1950

1995 95/46/EF Personverndirektivet, 24.10.1995

6.4 Forarbeider

6.4.1 Proposisjoner

Ot.prp. nr. 5 (2000-2001) Om lov om gjennomføring av straff mv. (straffegjennomføringsloven)

Ot.prp. nr. 102 (2004-2005) Om lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)

Ot.prp. nr. 75 (2006-2007) Om lov om utlendingers adgang til riket og deres opphold her (utlendingsloven)

Ot.prp. nr. 72 (2007-2008) Om lov om endringar i utlendingslovgivninga (reglar for EØS- og EFTA-borgarar o.a.)

Ot.prp. nr. 108 (2008-2009) Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)

Prop. 120 L (2013-2014) Om endringer i straffegjennomføringsloven mv. (Infoflyt-systemet mv.)

6.4.2 Rapporter

2012 INFOFLYT Informasjonsutveksling mellom politiet og kriminalomsorgen i saker med alvorlig kriminalitet og høy risiko. Rapport av 15. mai 2012 (Rapport 2012).

6.4.3 Norges offentlige utredninger (NOU)

1999 NOU 1999:27 «Ytringsfrihet bør finde sted», forslag til ny Grl. § 100

2003 NOU 2003:30 Ny offentlighetslov

2009 NOU 2009:1 Individ og Integritet

6.5 Rettspraksis

6.5.1 Høyesterett

Rt. 1975 s. 931

Rt. 1995 s. 530

Rt. 2006 s. 1300

Rt. 2007 s.1573

6.5.2 Den Europeiske menneskerettigehetsdomstol (EMD)

Handyside mot Storbritannia	saksnr. 5493/72 Strasbourg, 7.12.1976
Silver m.fl. mot Storbritannia	saksnr. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75 Strasbourg, 25.3.1983
Malone mot Storbritannia	saksnr. 8691/79 Strasbourg, 8.8.1984
Leander mot Sverige	saksnr. 9248/81 Strasbourg, 27.3.1987
Olsson mot Sverige	saksnr. 10465/85 Strasbourg, 24.3.1988
Peck mot Storbritannia	saksnr. 44646/98 Strasbourg, 28.1.2003

6.6 Andre myndigheters praksis

Ombudsmannssak 2007/2274	Undersøkelse av INFOFLYT-systemet i kriminalomsorgen

Ombudsmannssak 2007/264	7. Innsyn i dokumenter i INFOFLYT
Ombudsmannssak 2007/187	Lang saksbehandlingstid i kriminalomsorgen for permisjonssøknad – mangelfull orientering under sakens gang.
Ombudsmannssak 2006/1502	59. Kriminalomsorgens bruk av informasjon fra politiet i saker om permisjon og overføring til overgangsbolig.
Datatilsynet 07/01455	Kontrollrapport. Ila fengsel og sikringsanstalt.

6.7 Internasjonale rapporter

A/HRC/7/4/ Add.2 av 11.10.2007	Rapport fra FNs arbeidsgruppe mot vilkårlig fengsling (Working Group on Arbitrary Detention)

6.8 Litteratur

6.8.1 Bøker

Blixrud, Katrine Berg og Christine Ask Ottesen, Personvern i finanssektoren. Gyldendal Norsk Forlag AS 1.utg. Oslo, 2010.

Bruce, Ingvild og Geir S. Haugland, Skjulte tvangsmidler. Universitetsforlaget. Oslo, 2008.

Eckhoff, Torstein og Eivind Smith, Forvaltningsrett. Universitetsforlaget 9 utg. Oslo 2010.

Innjord, Frode A., Forvaltningsretten, I: Knophs oversikt over Norges rett. Universitetsforlaget 13.utg. Oslo, 2009.

Kjønstad, Asbjørn og Aslak Syse, Velferdsrett I Grunnleggande rettigheter, rettssikkerhet og tvang. Gyldendal Akademisk 4.utg. Oslo, 2010.

Løvdal, Jørgen, Informasjonsflyt i kriminalomsorgen – en studie i kontradiktorisk underskudd. Masteroppgave ved Universitetet i Oslo. Trykt i Juss-Buss' stensilserie nr. 120. Oslo 2011.

Robberstad, Anne, Sivilprosess. Fagbokforlaget 1.utg. Oslo, 2009

Schartum, Dag Wiese og Lee A. Bygrave, Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger. 2. utgave. Fagbokforlaget 2. utg. Oslo, 2011

Storvik, Birgitte Langset, Straffegjennomføring etter lov av 18.mai 2011 nr. 21. Høyskoleforlaget 2. utg. Kristiansand, 2011

Stub, Marius, Tilsynsforvaltningens kontrollvirksomhet. Undersøkelse og beslag i feltet mellom forvaltningsprosess og straffeprosess. Universitetsforlaget. Oslo, 2011.

Aall, Jørgen, Rettstat og menneskerettigheter. 2. Utgave. Fagbokforlaget. Bergen, 2007.

6.8.2 Nettdokumenter

Bernt, Jan Fridthjof. Kommentarer til offentleglova. I: Lovdatas nettsider [sitert 14.10.14]

Meidell, Merete. Kommentar til straffegjennomføringslova. I: Norsk lovkommentar nettversjon [sitert 14.10.14]
Schartum, Dag Wiese. Kommentar til personopplysningsloven. I: Norsk lovkommentar nettversjon [sitert 14.11.2014]

6.8.3 Annet

Regjeringens pressemelding av 25.6.2013 Nr. 79-2013 Kriminalomsorgsdirektoratet. http://www.regjeringen.no/nb/dep/jd/dep/underliggende-etater/kriminalomsorgsdirektoratet.html?id=426320 [lesedato 2.10.14]

Kriminalomsorgen.no: Straff i fengsel:
http://www.kriminalomsorgen.no/straff-i-fengsel.237611.no.html [lesedato 16.11.2014]

6.8.4 Samtaler

Jurist, Kriminalomsorgens region øst. Oslo 23.10.14

Ellertsen, Kim. Avdelingsdirektør (juridisk avdeling) i Datatilsynet. Oslo den 1.10.14.

Rønnevik, Cecilie. Juridisk fagdirektør i Datatilsynet. Oslo den 1.10.14.